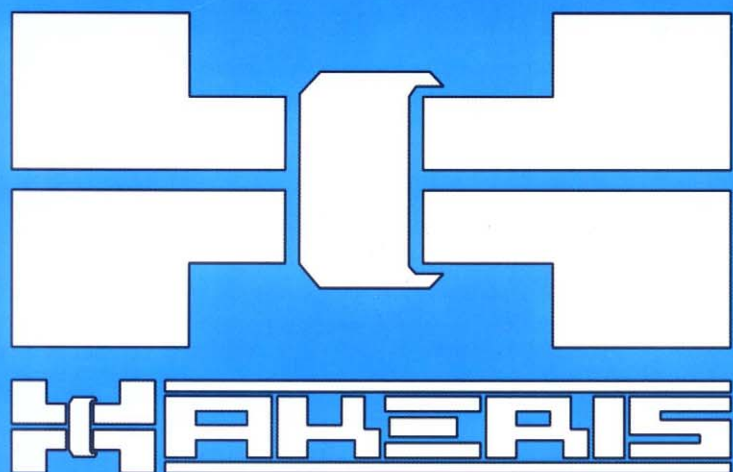
Tinklinis kamufliažas / Antivirusus į pamazgų duobę / Ne visos svetainės vienodai naudingos / Kalėjimas velniukui / Nevaikiškas triukas / Kaip grūdinosi „America Online“ / 100 tūkstančių tobulybės poligonų / Pramoninio šnipinėjimo technika / Kiekvienam servisui — kreiserinis greitis /

Nr. 12 (43) /2006



APSAUGOTA OS BE ANTIVIRUSŲ IR STABDŽIŲ

Kaina 9,99 Lt
Nr. 12 (43) '06
UP Computer Group

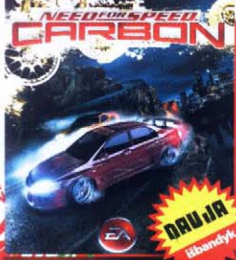


INFOC Pagalbos telefonas: 8 656 56000

Pašėlkim!

JAVA ŽAIDIMAI

10 Lt gera kaina

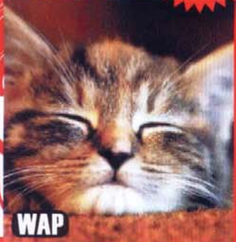


NAUJA išbandyk

Need For Speed : CARBON

Rašyk SMS: OHO JAVA 497689
Siųsk numeriu: 1354 10 Lt

Panasonic: VS3. Sagem: myC5-2, myV-55, myV-56, myV-65, myV75, myV-76, myX5-2, myZ-5. LG: tinka daugeliui modelių. Motorola: tinka daugeliui modelių. Nokia: tinka daugeliui modelių. Samsung: tinka daugeliui modelių. Siemens: CF75, CX65, CX70, CX75, ME75, S65, S75, SK65, SL75. Sony Ericsson: tinka daugeliui modelių.



Augink mielą kačiuką savo telefone!

Rašyk SMS: OHO JAVA 448533
Siųsk numeriu: 1354 10 Lt

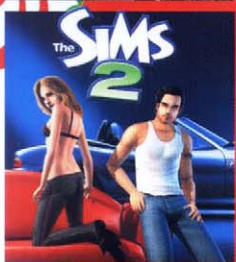
LG: KG800, KG810. Motorola: C975, E398, E550, PEBL U6, PEBL V6, L7, SLVR V8, V3 Razr, V400, V500, V525, V535, V547, V550, V551, PEBL V6, SLVR V8, V975, V980. Nokia: tinka daugeliui modelių. Samsung: tinka daugeliui modelių. Sharp: 902SH, TQ-GX1, TQ-GX25, V902. Sony Ericsson: tinka daugeliui modelių.



MEDAL of HONOR

Rašyk SMS: OHO JAVA 510672
Siųsk numeriu: 1354 10 Lt

LG: tinka daugeliui modelių. Motorola: C385, C390, C650, C975, C980, E1000, E1070, E398, E770, L2, L6, RAZR V3x, V1050, V180, V220, V3 Razr, V400, V500, V525, V535, V545, V547, V550, V551, PEBL V6, V980. Nokia: tinka daugeliui modelių. Samsung: tinka daugeliui modelių. Siemens: C65, C72, C75, CF75, CL75, CV65, CX65, CX70, CX75, M65, ME75, S65, S75, SK65, SL65, SL75, SP65. Sony Ericsson: tinka daugeliui modelių.



The Sims 2

Rašyk SMS: OHO JAVA 496422
Siųsk numeriu: 1354 10 Lt

Motorola: C380, E398, V220, V3 Razr, V500, V525. Nokia: tinka daugeliui modelių. Samsung: D500, D600, D820, E330, E700, E710, E720, E730, E760, E800, X450, X460, X640, X640C, X660, Z140, Z300, Z500. Siemens: C65, CL75, M65, S65. Sony Ericsson: J300i, K300, K300i, K500i, K600i, K608i, K610i, K700, K750i, K800i, S700i, T610, T630, W300i, W550i, W800, W800i, W900i, W950i, Z1010, Z520i, Z530i, Z600, Z610i, Z800.

MP3 MELODIJOS

WAP

Rašyk SMS: **OHO RT kodas** pvz.: **OHO RT 275705** Siųsk nr.: **1350**
Siųsk draugui: **OHO RT kodas 3706XXXXXXX** Siųsk nr.: **1350** 5 Lt

69 danguje * Gyvenu !!!NAUJA!!!	510967
Sniegė & Karina * Ten !!!NAUJA!!!	511012
Naujieji Lietuviai * Princesė !!!NAUJA!!!	510979
Vaidas * Myliu !!!NAUJA!!!	510974
Jurga * Nebijok !!!NAUJA!!!	510976
Naujieji lietuviai * Ruri ruri	275707
Naujieji lietuviai * R1	275705
Naujieji lietuviai * Afigienai	275701
Naujieji lietuviai * Užknisa tavo skambučiai	275700
69 danguje * Super mergaitės	275712
69 danguje * Ruri ruri	275711
69 danguje * 9 danguj	275709
SEL feat. MIA * Muzika	275748
SEL * Parašyk man laišką iš Paryžiaus	275696

Tikro garso melodija gali būti mp3 arba amr formatu, tai priklauso nuo telefono modelio. Tinka: Motorola: A1000, A630, A780, A835, A920, A925, C261, C380, C385, C390, C650, C975, C980, E1, E1000, E1070, E365, E378i, E398, E550, E680, E770, E790, L2, L6, MPx220, PEBL U6, PEBL V6, RAZR V3x, ROKR E1, L7, V8, V1050, V180, V188, V190, V220, V235, V3 Razr, V400, V500, V501, V505, V525, V535, V545, V547, V550, V551, V555, PEBL V6, V710, SLVR V8, V975, V980. Nokia: 2610, 2650, 3152, 3155, 3200, 3220, 3230, 3250, 3300, 3600, 3620, 3650, 3660, 5140, 5500, 6020, 6021, 6060, 6070, 6080, 6101, 6102, 6103, 6111, 6125, 6131, 6136, 6151, 6170, 6200, 6220, 6230, 6233, 6234, 6235, 6255, 6260, 6270, 6280, 6288, 6600, 6630, 6670, 6680, 6681, 6820, 7200, 7260, 7270, 7280, 7360, 7370, 7380, 7600, 7610, 7650, 7710, 8800, 8801, 9300i, 9500, E50-2, E60-1, E61-1, E70-1, N-Gage, N70, N71, N72, N73, N80, N90, N91, N92. Samsung: A920, C240, D300, D520, D720, D730, D800, D820, D830, D840, D900, E316, E317, E320, E335, E338, E350, E370, E530, E600, E608, E610, E620, E640, E720, E770, E780, E860V, E900, E910, P207, P300, P777, P850, P900, P910, T309, X300, X500, X620, X630, X660V, X670, X680, X700, X810, X820, Z110, Z130, Z140, Z140V, Z150, Z300, Z400, Z500, Z510. Sony Ericsson: B200, D750i, F500, J210, J220i, J300i, K300i, K310i, K500i, k508i, K510i, K600i, K608i, K610i, K700, K750i, K790i, K800i, M600i, P900, P910, P990i, S600i, S700i, T123i, T290, T616, T618, T628, T68, V600i, V630i, V800, W300i, W550i, W600i, W700i, W710i, W800i, W810i, W850i, W900i, W950i, Z1010, Z300i, Z520i, Z530i, Z550i, Z610i, Z710i, Z800.

MELODIJOS

2 Lt gera kaina

SUPER SMAGIOS ŠVENTĖS

Coca-Cola Christmas	53652
Merry Xmas - War Is Over	34494
Cheeky Girls * Have A Cheeky Christmas	34492
Tomas Augulis * Kalėdų naktį tylią	34242
Santa Claus Is Comming To Town	26623
Jingle Bells	26564
Schubert * Ave Maria	9634
George Michael * Last Christmas	9631
"V lesu rodylas jolacka"	58024

SUPER MELODIJŲ TOP10

Dima Bilan * Never Let You Go	218439
A.Rimiškis * Kartais būna	214389
Lordi * Hard Rock Hallelujah	218458
Bumer 2 * Osen	221626
69 danguje * Devintam danguj	216344
Vilija * Mylėk	206288
69 Danguje * Super mergaitės	222321
Raketa * Dolce Gabana	216342
LT United * We Are The Winners	218462
Paris Hilton * Stars Are Blind	219247

SUPER MELODIJŲ NAUJIENOS

Red Hot Chili Peppers * Tell Me Baby	225475
Fergie * London Bridge	225608
Reamonn * Tonight	225674
Robbie Williams * Rudebox	225532
Robbie Williams * Lovelight	481791
Bob Sinclar * Rock This Party	225722
Nelly Furtado * Promiscuous	221190
Justin Timberlake Ft T.I. * My Love	483301
Shakira Ft Carlos Santana * Illegal	209869
Rihanna * We Ride	497553
Bodyrox * Yeah Yeah	218923
Akon Ft Eminem * Smack That	481532
Fedde Le Grand * Put Your Hands Up 4 Detroit	497552
Westbam * United States Of Love	225632
"Kalėjimo bėglys" filmo garso takelis	498288
Bumer 2 * Osen	221626
Paris Hilton * Stars Are Blind	219247
A. Mamontovas * Viskas iš naujo	222420
Sel ft. Mia * Muzika	211815
69 Danguje * Super mergaitės	222321
Mango * Ejom	222324

SUPER MELODIJŲ REKOMENDACIJA

Shakira/W.Jean * Hips Don't Lie	213723
Eminem/Nate Dogg * Shake That	201846
Gnarls Barkley * Crazy	211667
Dima Bilan * Eto bila liubov	222323
Flipsyde * Trumpets	219363
Tyla [kai ko nors nenori girdėti]	57532
Bob Sinclar * World, Hold On	214526
Eminem * Welcome 2 Detroit	21308
Skamp * Thinking about you	222404
James Brown * Sex Machine	206028

KAIP GAUTI MELODIJĄ? WAP 2 Lt

POLI melodija - rašyk SMS: **OHO SUPER kodas**
pvz.: **OHO SUPER 219363** Siųsk numeriu: **1352**
Siųsk draugui: **OHO SUPER kodas 3706XXXXXXX**
Mono melodija: **OHO M kodas** Siųsk numeriu: **1352**

POLI melodijos tinka:

Polifoninės melodijos tinka: Nokia: visiems naujiems telefonams. Samsung: D500, E700, E710, P400, P510, S300M, SGH-E330, E800, E810, X450, X460, T100, V200, X100. Siemens: A60, C55, C60, C62, CF62, CV65, CX65, CX70, M55, M65, MC60, S55, S65, SK65, SL55, SL65, ST60, Sx1. Sony Ericsson: K500i, K700, K750, W800i, P800, P900, P910, S700i, T230, T290i, T300, T310, T610, T630, V800, Z1010, Z200. **Mono melodijos tinka:** Nokia: visiems naujiems telefonams.



Vakar bandžiau prisiminti kada paskutinį kartą pirkau kokį nors žurnalą. Nepavyko.

Bandžiau prisiminti, kada paskutinį kartą skaičiau kokį nors žurnalą. Pavyko prisiminti prieš tris mėnesius pavartyta vieną lietuvišką žurnalą ir padėtą su mintimi „kai turėsiu laiko — paskaitysiu". Po mėnesio gavau to paties žurnalo kitą numerį, kurį padėjau ant senojo su ta pačia mintimi. Ne, tai ne dėl to, kad aš nemėgčiau skaityti ar neturėčiau tam laiko. Nuolat jaučiu poreikį naujai informacijai, bet vis dažniau jos ieškau internete, o ne bibliotekoje ar žurnalų puslapiuose. Priežastys labai paprastos: informacijos daug, lengvai randama, o svarbiausia — čia ir dabar. Nereikia laukti mėnesį naujojo numerio, nereikia bėgti per lietų į spaudos kioską ir ten nerasti laukiamo žurnalo. Bandant surasti tai, ką jau skaitei prieš pusę metu, nereikia lįsti po lovą ir bandyti dulkių krūvoje ieškoti reikiamo žurnalo numerio, o tada pervertus visų žurnalų visus puslapius, prisiminti, kad būtent tą numerį paskolinai kaimynui, o jis paliko jį pas močiutę kaime.

Leisk pateikti dar vieną iliustratyvų pavyzdį: ką darai niekaip negalėdamas rasti kambaryje savo mobiliojo telefono? Teisingai, skambini savuoju numeriu iš kito telefono. O jei nerandi raktų, piniginės ar akinių nuo saulės? Pastarieji ypač reikalingi šią žiemą... Bet grįžkim prie esmės. Jei realiame gyvenime būtų CTRL+F ar ALT+F7 (čia kaip kam patogiau) mygtukai, nebereikėtų versti visko iš eilės ieškant už lovos užkritusių raktų ar skalbinių dėžėj miegančio katino. Nepakenktų tokie mygtukai ir žurnalo puslapiuose, tik deja, dar niekas nesumastė kaip jų padaryti. Išeitis yra: žurnalas skaitmeniniame formate virtualioje erdvėje.

Praėjusiame numeryje klausėme, ar nori skaityti „Hakerį" internete. Beveik 6 % atsakė neigiamai. Ką gi, patys norėjot. Popierinis „Hakeris" su jumis atsisveikina, o mes einam gaminti jį virtualioje erdvėje.

untitled

06



10



15



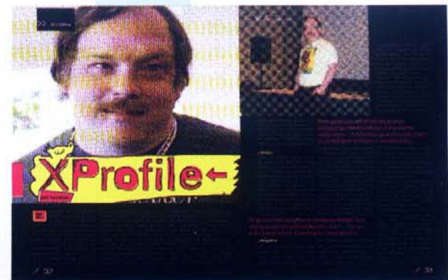
20



26



32



34



36



42



TURINYS 12(43)

Žurnalas „HAKERIS“
ISSN 1648-6862

Jonavos g. 254a, LT–44132 Kaunas
http://www.hakeris.lt
root@hakeris.lt

Vyr. redaktorius
Arnaldas Augutis
Dizaineris–maketuotojas
Gediminas Lukavičius
Stilistė
Laura Barzdaitienė

REDAKCIJA:
Jogintas Visockas,
Žydrūnas Kliševičius,
Edmundas Valaitis,
Kristina Dembinskaitė,
Aurelija Pociūtė,
Ričardas Jaščemskas,
Teresė Štuopytė.

LEIDĖJAS:
UAB „InDiza“
Jonavos g. 254a,
LT–44132 Kaunas
Tel.: +370 37 763 203
Faks.: +370 37 764 995

Dėl reklamos žurnale kreiptis:
Stasys Švabas
Mob. tel.: +370 614 16659
+370 5 210 1520
Fax. +370 5 210 1521
stasys@upg.lt

SPAUDĖ:
AB spaustuvė „Spindulys“
Gedimino g. 10,
LT–44318 Kaunas
Užs. Nr. 6.1212
Žurnalas parengtas bendradarbiaujant
su kompanija
„GameLand International, Inc.“

46



52



56



60



62



67



→ MAKDONALDO TROJANAI

„McDonalds" nūnai maitina visą pasaulį, o Japonijoje tai iš viso jau kone nacionalinis maistas. Ten nuolatiniams lankytojams net rengiami konkursai su dovanomis. Neseniai kompanija „Coca–Cola" ir „McDonald's" Japonijos filialas suorganizavo reklamos akciją, kurios metu mėsainių mėgėjams buvo už dyką dalinami skaitmeniniai grotuvai. Tačiau mėsainių ėdrūnai džiaugėsi neilgai: paaiškėjo, kad šie grotuvai pateikiami su siurprizu. Tiksliau šnekant — su trojanu *QQpass spyware*, kuris slypėjo tarp 10–ties įrašytų garso kūrinių. Ar verta sakyti, kad apie tai sužinoję japoškės pakėlė triukšmą ir už tai grasino iš savo meniu amžiams išbraukti skrudintas bulvytes su didele kolos porcija. Tačiau „McDonalds" — gudrūs, jie tuojau pat atsiprašė bei pranešė, kad įvyko nesusipratimas, bei painstruktavo liaudį, kaip kompiuterį išgydyti nuo užkrato, o visi grotuvai, kurie dar nespėjo pakliūti į apsirijėlių rankas, buvo skubos tvarka atšaukti iš prekybos. Šios istorijos moralas toks: „nemokamas sūris būna tik pelėkautuose" ir „laikykis toliau nuo *McDonalds*".

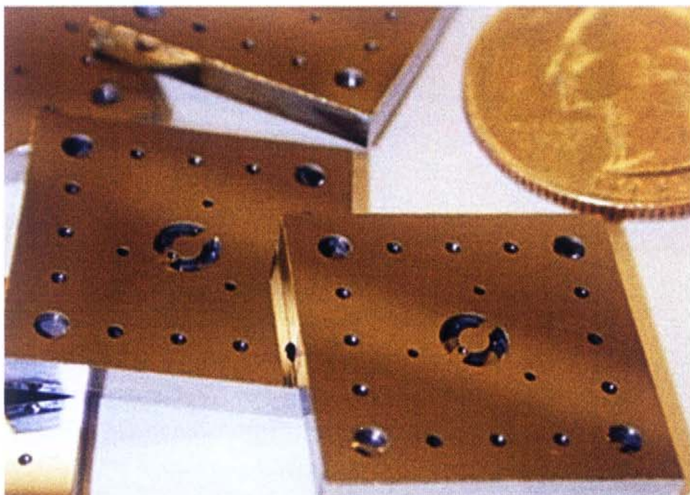
→ MERGAITĖ IR BUŠAS

JAV specialiosios tarnybos eilinį kartą siautėja. Spalio mėnesį vyko vos ne operacija „Audra dykumoje", kurios metu tiesiog mokyklos pastate buvo sulaikyta 14–os metų mergaitė. Mažytė strazdanota Džulija visai neprekiavo narkotikais ir nesprogdino Pentagono, o viso labo pasauliniame voratinklyje paliko karikatūrą su priešmirtinėse kančiose besiraitančio prezidento nuotrauka ir užrašu: „Nužudyti Bušą". Ir šiaip visas puslapio turinys bylojo apie akivaizdžią autorės nemeilę dėdulei Bušui. Per biologijos pamoką vaiką areštavusios ir jį su dideliu pasimėgavimu apklaususios specialiosios tarnybos išsiaiškino, kad Džulija neruošė jokio sąmokslo, nesiruošė samdyti kilerio ir viso labo nemėgsta savo šalies prezidento. „Jūs ką, aš labai taiki mergaitė ir klausau mamytės", — prisipažino mažoji išdykėlė. Lemtingasis puslapis buvo saugomas nemokamo hostingo *myspace.com* serveryje, kurį gerai paieškojęs tu tikrai surasi.

KILL BUSH

→ ICANN — TREČIAS NEREIKALINGAS?

Teisminės aistros tarp tinklo kompanijų verda visur. Dabar vienas iš garsiausių konfliktų užviręs tarp „E360Insight" ir „Spamhaus". Pirmoji legaliai užsiima komercine reklama internete, o antroji tvarko juoduosius spamerių sąrašus ir blokuoja iš šių adresų siunčiamą elektroninį paštą. Kai šiame black–list'e atsidūrė „E360Insight", jai tai labai nepatiko. Firma net pateikė teismui reikalavimą išmesti savo gerą vardą iš niekingųjų spamerių bazės ir kaip moralinę kompensaciją sumokėti beveik 12 milijonų dolerių. Kadangi „Spamhaus" yra Didžiojoje Britanijoje, o teismas vyko JAV, antispameriai atsisakė paklusti teismo sprendimui: atseit, jūsų įstatymai čia negalioja. Amerikiečių juristai pasipiktino tokiu nepaklusnumu ir pažadėjo iš viso uždaryti antispamerių kontorą. Tam „E360Insight" susisiekė su ICANN — tarptautine organizacija, užsiimančia domenų vardų paskirstymu internete, bei paprašė sustabdyti jiems neįtikusios svetainės darbą. Šie teismo sprendimai forumuose sukėlė daugybę diskusijų. Žmonės mano, kad ICANN neturėtų kištis į dviejų pusių konfliktą, kadangi jos užduotis — valdyti visą domenų vardų sistemą, o ne atskirus vardus. ICANN paklusimas „E360Insight" ir teismo sprendimui būtų vertinamas kaip priklausomybė nuo JAV. Ar ši organizacija paprieštaraus Amerikai, ar išsaugos savo neutralitetą — apie tai sužinosi kitame mūsų numeryje!



→ MONETOS DYDŽIO BATERIJA SU DUJŲ TURBINA

Tyrinėtojai iš Masačūsetso technologijos instituto padarė praktiškai neįmanoma — jie sukonstravo miniatiūrinę bateriją, kuri energiją generuoja su... dujų turbina! Mikroskopinė turbina įkelta į silicio mikroschemą, kuri kiek didesnė už amerikietiškų 25 centų monetą. Be to, kaip parodė testai, dujinė baterija gali dirbti 10 kartų ilgiau už savo elektrinį analogą. MIT mokslininkai panaudojo pačius naujausius MEMS (*Micro-Electro-Mechanical Systems*) sistemų srities pasiekimus. Turbinos mentės pagamintos iš specialios ypač tvirtos medžiagos, kuri leidžia turbinai veikti dideliu greičiu — 20000 apsisukimų per sekundę. Pati turbina — gana sudėtinga mikrosistema. Ji susideda iš šešių tarpusavyje sujungtų silicio plokštelių. Kiekviena turbinos plokštelė — tai ištisas kristalas su „į eilę sustatytais" atomais, dėl ko jis išsiskiria ypatingu tvirtumu. Gaminant šio motoro komponentus, kiekviena plokštelė buvo individualiai apdorojama, kad būtų pašalintos nereikalingos medžiagos. Tarp plokštelių įsikūręs turbinos mechanizmas. Iš pradžių pagaminamas silicio „vaflis", iš kurio išpjaunama 80–100 detalių. Tada šis „vaflis" supjaustomas ir iš silicio mazgų surenkama dujų turbina, kurios nominali galia siekia 10 Vatų. Mažytėje degimo kameroje sumaišytas kuras ir oras dega plieno lydymosi temperatūroje. Nedidelis kompresorius suspaudžia orą ir užtikrina aušinimą: dalis oro nukreipiama ne į degimo kamerą, o į turbinos korpuso ertmes. Mokslininkai planuoja sukurti nešiojamajam kompiuteriui skirtos baterijos prototipą, kuris leistų portatyvinius kompiuterius padaryti iš tiesų mobiliais.

→ IŠ PATRANKOS Į... ŽEMĖS ORBITĄ

Viena iš kosmoso inžinerių užduočių — efektyvių ir nebrangių krovinių pristatymo į orbitą būdų sukūrimas. Dar užpraeito amžiaus pabaigoje Žiulis Vernas siūlė paprastą kosminių kelionių būdą: kosminius aparatus iššauti iš patrankos. Žinoma, toks būdas nėra skirtas kosmoso turizmui, tačiau lengvų palydovų pristatymui — pats tas. Elektroninės patrankos–greitintuvo kūrimu užsiėmė amerikiečių karinės oro pajėgos, kurios finansuoja ypač lengvų palydovų paleidimo sistemos projektą. Tačiau „Magnetic satellite launch system" — tai visai ne patranka, o milžiniškas žiedas, savo sandara primenantis elementariųjų dalelių spartintuvus, kurie padeda fizikams atskleisti gamtos paslaptis, tiktai čia vietoje dalelių šis žiedas spartins nedidelį konteinerį su sviediniu, kurio viduje bus dešimties kilogramų palydovas. Iš pradžių inžinieriai sukurs sumažintą sistemos prototipą, kurios žiedo skersmuo būtų apie 50 metrų. Galutinai viską realizavus šio komplekso iš superlaidžių elektromagnetų, kurie išlaikytų ir paspartintų konteinerį su palydovu, žiedo skersmuo turėtų siekti 2 kilometrus.

Palydovą planuojama įkelti į kūgio formos sviedinį, sudarytą iš labai masyvaus volframo antgalio su naudingam kroviniui skirtu skyriumi, raketinio variklio skyriaus, kuro bakų ir oksidatoriaus. Spartinimo žiede pabaigoje palydovą veiks 10 tūkstančių g siekianti išcentrinė jėga, tačiau valdomuose sviediniuose sumontuota elektronika šūvių metu išlaiko 20 tūkstančių g perkrovas. Taigi tikrai įmanoma sukurti mažyčius palydovus, kurie gali išlaikyti tokias perkrovas.



→OPTINIS TAIKIKLIS TERORISTUS ATPAŽĮSTA IŠ VEIDO



Greitai sunkus karštuosiuose planetos taškuose su tarptautiniu terorizmu kovojančių šauniųjų amerikiečių jūrų pėstininkų darbas taps žymiai lengvesnis. Snaiperiui tereikės taikiklį viso labo nukreipti į įtartiną žmogų, o „protinga" elektronika atpažins teroristą ir sukomanduos „Ugnis!". Sistemą kuriančios kompanijos ACAGI generalinis direktorius apie naująjį projektą kalba taip: „Kareiviai turi ant automatų arba šalmų sumontuotas vaizdo kameras, tačiau tai tik viena pusė. Juk ši aparatūra nieko neatpažįsta. O mūsų sistema, pamačiusi ką nors pažįstamo, apie tai praneša, kas leidžia greitai priimti sprendimus". Į sistemą bus iš anksto užkrautos potencialiai pavojingų asmenybių nuotraukos. Tai padaryti pakankamai paprasta, kadangi specialiosioms tarnyboms pagrindiniai teroristai yra žinomi.

IAECS (*Image Acquisition and Exploitation Camera System*) sistemos smegenys — tai 900 gramų sveriantis ant juosmens tvirtinamas kompiuteris. Vaizdo kamera montuojama arba ant šalmo, arba kartu su optiniu taikikliu. Pastaruoju atveju galima elektronikai tiksliai nurodyti žmogų, kurį reikia patikrinti. Pirmieji kišeninių IAECS įrenginių pavyzdžiai turėtų pasirodyti iki šių metų pabaigos. Tai bus pirmoji pasaulyje mobili ir visiškai autonominė asmenų atpažinimo realiu laiku sistema.



→Į KOSMOSĄ UŽ 200'000 DOLERIŲ

Šiandien norint išskristi į kosmosą reikia už tai palikti nuo vieno iki keliolikos milijonų dolerių, tačiau artimiausiu metu tapti kosmoso turistu bus galima už viso labo... 200 tūkstančių dolerių. Tokį kainų nuosmukį gali sukelti privataus kosminio aparato *SpaceShipTwo* (SS2) sukūrimas.

„Virgin" imperijos vadovas Ričardas Brensonas *NextFest* festivalyje ir tradiciniame amerikiečių žurnalo „Wired" forume apie tai surengė prezentaciją. Žiūrovams buvo parodytas virš scenos plevenantis kosmoplanas *SpaceShipOne* ir po juo prisišvartavęs natūralaus dydžio jo įpėdinio maketas su atlapotu dešiniuoju bortu.

Naujasis SS2, kuris taip pat žinomas kaip *VSS Enterprise*, priešingai nei SS1, suprojektuotas išskirtinai kosmoso turizmui. Dėl to šis laivas maždaug 3 kartus stambesnis už savo pirmtaką, jame telpa 8 žmonės: 6 keleiviai (salone yra 2 eilės po 3 krėslus) ir 2 pilotai (nuo salono atskirtoje kabinoje).

SpaceShipTwo, kaip ir antrosios kartos lėktuvą–spartintuvą — *WhiteKnightTwo*, kuris pakels SS2 į 18,2 tūkstančių metrų aukštį, — kuria Berto Rutano (pastarasis gerai žinomas visame pasaulyje dėl to, kad suprojektavo be nusileidimo visą Žemės rutulį apskridusį lėktuvą) kompanija „Scaled Composites", tiksliau šnekant, jos „dukrelė" *Spaceship Company*.

Suborbitiniai 2,5 valandos trunkantys turistų skrydžiai į 110–140 kilometrų aukštį numatyti 2009 metų pradžiai, o aparatai bus paleidžiami iš naujojo kosmodromo Niu Meksike. Po 12 mėnesių kosmoso lėktuvas atliks bandomuosius skrydžius. Tuomet ir bus nuspręstas kosmoso turistų likimas.

KORPUSAS BE VARŽTŲ

KOMPANIJA „CHIEFTEC" PRISTATO NAUJĄ „MESH" SERIJOS KORPUSĄ CH-01B-B-SL-OP. ŠI PRAILGINTA „MIDITOWER" VERSIJA SU USB/„FIREWIRE"/AUDIO PRIEVADAIS APJUNGIA SAVYJE DAUGELĮ VARTOTOJŲ PAGEIDAVIMŲ IR FIRMINIŲ KOMPANIJOS NAUJOVIŲ.

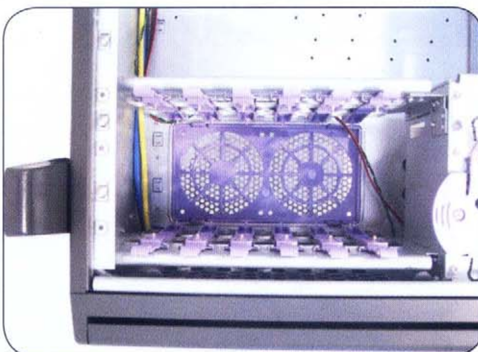
Joks kitas „Miditower" korpusas neleis jums įrengti ne tik ATX, bet ir EATX sisteminės plokštės, taip pat net 6 kietųjų diskų bei 5 aušinimo ventiliatorių. Jums siūlomas dviejų klasikinių dizainų pasirinkimas: juodas arba juodas su sidabriniu priekiniu skydeliu.

Kitas naujo modelio ypatumas – galimybė įrengti išorinius diskų įrenginius be jokių tvirtinimo varžtų. Tik jūsų naujas korpusas, diskų įrenginys (CD, DVD, FDD ir kt.) bei jūs. Taip patentuota pavažų („rails") konstrukcija leidžia atlikti kietojo disko fiksaciją be varžtų, tuo pačiu užtikrindama jo praktiškai begarsį veikimo procesą bei neleisdama vibruoti visam korpusui.

Taip pat yra du lengvai prieinami USB 2.0 prievadai, viena „IEEE 1394 Firewire" jungtis bei audio prievadas – visi jie išdėstyti priekinės sienelės dešinėje pusėje.

PCI plokščių tvirtinimas atliekamas taip pat be varžtų, panaudojant fiksatorių, o dešinėje sienelėje esanti rankenėlė padės lengvai ir greitai atidaryti korpusą.



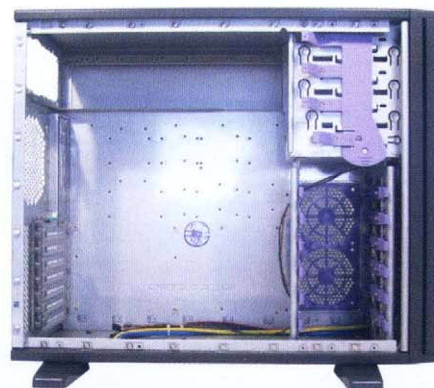


Išorinio DVD diskų įrenginio instaliavimas: atitraukti fiksatorių, įdėti diskų įrenginį, paleisti fiksatorių.

Atvirkščiam procesui pakanka atitraukti fiksatorių ir tuo pačiu metu nuspausti diskų įrenginį.



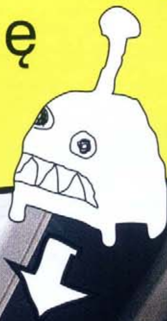
Korpusas be kairiojo skydelio: šešios HDD skirtos sekcijos, microATX, ATX ir EATX tipo motininių plokščių tvirtinimo vieta.





„Mesh" serijos korpuso CH-01B-B-SL-OP charakteristikos:	
Korpuso tipas:	micro ATX, ATX (CEB 1.01), EATX (SSI EEB3.x)
Išmatavimai (Ilgis x Plotis x Aukštis):	ω 540mm x 205mm x 460mm* *=su kojelėmis (be kojelių - 442mm)
Svoris:	w15 kg, su maitinimo bloku
Išoriniai įrenginiai:	w3x5 1/4", 1x 3,5"
Vidiniai įrenginiai:	w6 sekcijos, skirtos 3,5" HDD
Maitinimo blokas:	w400Wt, ATX 2.0
Jungtys priekiniame panelyje:	wdu USB 2.0 prievadai, viena „IEEE 1394 Firewire" jungtys, audio prievadas

anti VIRUSĄ//
į pamazgų duobę



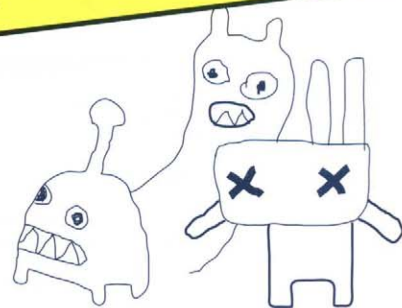
KAI KURIE ANTIVIRUSĄ PRIIMA KAIP NEATSIEJAMĄ OPERACINĖS SISTEMOS DALĮ IR TIESIOG NEĮSIVAIZDUOJA SAVO EGZISTAVIMO BE SKIRTINGŲ GAMINTOJŲ APSAUGINIŲ PAKETŲ, KURIE LAISVAI PRALEIDŽIA UŽKRATĄ, TAČIAU ŽIAURIAI STABDO DARBĄ IR SUKELIA IŠTISĄ KONFLIKTŲ VIRTINĘ IKI PAT BSOD PASIRODYMO. PATS GERIAUSIAS ANTIVIRUSAS — TAI PATI OS! TEREIKIA IŠMOKTI TEISINGAI JA NAUDOTIS!

APSAUGOTA OS BE ANTIVIRUSŲ IR STABDŽIŲ

Antivirusai — už galimybių ribų

Antivirusai šiuo metu praktiškai visiškai prarado savo ankstesnį reikšmingumą ir atkakliai bando pasitraukti nuo prarajos, kurios dugne jie yra. Taip yra dėl to, kad vykdomas bylas užkrečiantys virusai per pastaruosius keletą metų faktiškai išnyko. Be to, uždrausti rašymą į vykdomas bylas panaudojant operacinės sistemos priemones galima kur kas paprasčiau, pigiau, greičiau ir patikimiau, negu įdiegti antivirusinį paketą. Ir visiškai beprasmiška bandyti gydyti užkrėstus objektus, juk bet kuriuo metu juos galima atstatyti iš distributyvo kopijos, saugomos CD-R/RW diske arba parsisiųstos iš interneto. Antiviruso monitorius, stebintis visas kuriamas/atidaromas bylas ir tikrinantis jas veikimo metu — tai papildomas stabdymas (kartais net labai žymus),





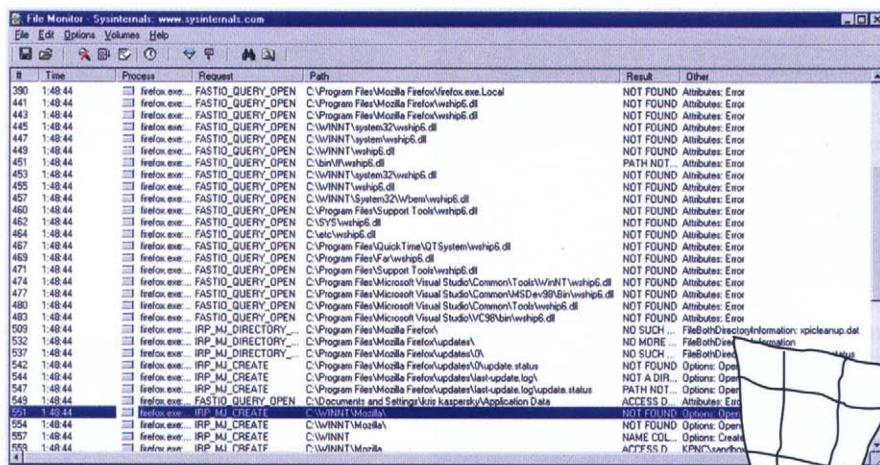
panašaus, tuomet šie algoritmai padarys išvadą, kad čia susidurta su programa, kuri gali įsiterpti į kitus procesus, kas yra akivaizdus kirminų ir derintuvų požymis. Situaciją smarkiai apsunkina tai, kad daugelį virusų metodų dabar aktyviai naudoja protektoriai, todėl jeigu tik mes nenuraminsime euristikos, jie susidoros su gera puse legalių programų, ko jokiu būdu negalima leisti! Ir šiaip, jeigu viruso kūrėjas yra nekvailas žmogus, tuomet jis savo produktą daug kartų perleis per pačias įvairiausias euristikas, taip pasiekdamas visiško ir besąlygiško jų kapituliavimo.

Kalbant apie kirminus (taip pat ir plačiai nuskambėjusį MS BLAST, kuris dar žinomas kaip Love San), tai čia iš viso fantastika. Ar antivirusai juos pašalina, ar ne — kas iš to? Kol egzistuoja neužtaisyta sistemos saugumo skylė, kirminas lyg feniksas vėl ir vėl pakils iš pelenų. Be to, visada yra tikimybė, kad kas nors protingas parašys savą shell–kodą, kuris su MS BLAST neturi nieko bendro, dėl ko jo neaptiks joks antivirusas! Kai kurias skyles galima uždaryti su ugniasiene, tačiau bendru atveju tam reikia įdiegti pažeidžiamo produkto (kuriuo gali būti tiek pati OS, tiek ir bet kuris jos komponentas: IE, FireFox ir t.t.) gamintojo pataisymą.

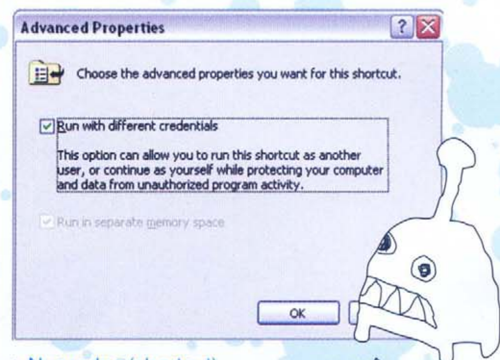
Yra ir toks antivirusų tipas, kaip revizoriai, kurie tikrina egzistuojančių bylų vientisumą ir kontroliuoja naujai sukurtas. Kai kurie revizoriai kontroliuoja ir sisteminį registrą, ypač tas šakas, kurios tiesiogiai ar netiesiogiai atsako už automatinį programų paleidimą. MS–DOS laikais tai buvo labai geras dalykas, tačiau dabar kietieji diskai taip išsipūtė, kad skenavimo procedūra

konfliktai, kritinės klaidos, mėlynieji mirties ekranai ir dar visokia papildoma bei niekuo nepateisinama knisalynė. Visa problema tame, kad antivirusas gali gaudyti tik tuos virusus, kuriuos jis pažįsta, o virusus dabar rašo visi, kas tik netingi, todėl net ir su nepaprastai ypatingu operatyvumo lygiu mes neturime jokios garantijos, kad visi užkratai bus atpažinti. Be to, su šiek tiek pataisyta kieto protektoriaus versija supakuotas virusas turi 100% galimybes likti nepastebėtas! Sudėtingi protektoriai su centrinio procesoriaus emuliatoriumi jau neišpakuojami, o norint su jais susidoroti reikia statinio išpakuotuvo, įeinančio į antiviruso bazės „varikliuką“ ir susidorojančio tik su griežtai konkrečiomis protektorių versijomis bei labai liguistai reaguojančio net į nežymius supakuotos bylos struktūros pakeitimus. Ką ten struktūra! Paprastai pakanka į įėjimo tašką įdiegti perėjimą (jump) į emuliatoriui nežinomą instrukciją (pavyzdžiui, į ką nors iš SSE/SSE2 rinkinio), ir antivirusai bandydami įveikti tokį riešutėlį išsilaužo dantis, kadangi kintamas x86 instrukcijų ilgis jam neleidžia nustatyti kitos mašininės komandos pradžios!

Beje, net jeigu antivirusui pavyktų įveikti pakuotuvą ir supakuotą kodą perduoti euristiniams algoritmams, jis ten vis tiek neaptiktų jokių virusų požymių, nebent tai bus vaikiško lygio antivirusas. Nešifruotos tekstinės eilutės su registro raktais, atsakingais už automatinį paleidimą kartu su OS, antivirusų vykdomų bylų pavadinimai, „rm –rf /“ stiliaus komandos su didele tikimybe byloja apie kenksmingą programą, tačiau visa tai galima labai lengvai užšifruoti. Euristiniai algoritmai taip pat gali analizuoti importo lentelę ir funkcijai GetProcAddress perduodamus argumentus. O jeigu ten pasitaikys WriteProcessMemory, VirtualAllocEx, CreateRemoteThread arba kas nors



› Bylų monitorius rodo, kur sutrinka Ugninės Lapės paleidimas



› Nuorodos (shortcut) savybėse sukonfigūruojame paleidimą kito vartotojo vardu

trunka daugybę laiko. Be to, daugelyje skenerių paliktos klaidos, leidžiančios bylas užkrėsti nepakeičiant jų kontrolinės sumos, jau nė nekalbant apie tai, kad naudojant teisingą priėjimo kontrolės politiką (paprasčiau šnekant, ACL'us) prarandamas tokių skenerių aktualumas, juo labiau, kad pradedant W2K operacinė sistema pati su SFC (System File Checker) mechanizmu kontroliuoja gyvybiškai svarbių bylų vientisumą. Čia esmė tokia. Paleidus komandą „sfc /scannow" šis sisteminis įrankis pradeda nuosekliai tikrinti sisteminių bylų vientisumą. Susidūrus su bet kokiomis problemomis įtartinas bylas pakeis tikrosios keše (%SystemRoot%\WINDOWS\System32\Dllcache\) saugomos jų kopijos. Na štai, dabar kas nors pasakys, kad SFC lengva apgauti... Tačiau ir skenerį apgauti nė kiek ne sudėtingiau, ypač jeigu virusas slepiasi branduolio lygyje arba iš viso neįsiterpia į jokius failų sistemos objektus, egzistuodamas tik virtualioje kokio nors proceso atmintyje. Procesų virtualios atminties vientisumą kontroliuoti imasi tiek antivirusai, tiek ir asmeninės ugniasienės, kurios atpažįsta ir užkerta kelią visiems žinomiems įsiterpimo į svetimą adresų erdvę būdams, tačiau šis mechanizmas veikia šiaip sau. Su sumažintomis privilegijomis paleistam kenksmingam kodui priėjimą prie svetimų procesų galima uždrausti su pačios operacinės sistemos priemonėmis, o su administratoriaus teisėmis paleistas kodas per visus apsaugos lygius praeis kiaurai kaip per sviestą (su ta sąlyga, kad jį rašė ne koks nors pradinukas, o bent kiek patyręs žmogus). Nemaloniausia tai, kad yra daugybė legalių programų, pavyzdžiui, daugialypės terpės klaviatūrų ir pelių, kurios įsiterpimą į svetimą adresų erdvę naudoja savo multimedijos galimybėms realizuoti, taigi dėl aklų ugniasienės/antiviruso draudimų tokie prietaisai neveiks! Tai reiškia, kad vartotojui reikia suteikti teisę rinktis. O ar jis galės atskirti gerą programą nuo blogos? Vis dėlto čia baisiausia net ne tai. Kuo giliau ugniasienė/antivirusas įsiskverbia į sistemą, tuo sudėtingiau kenksmingam kodui jį apeiti, tačiau tuo daugiau konfliktų ir klaidų jie (ugniasienės bei antivirusai) sukelia.

Taip išeina, kad protingai sukonfigūruotoje sistemoje nereikia jokio antiviruso, o su kreiva konfigūracija nepadės joks antivirusas (ugniasienę verta įdiegti tik tam, kad naminį lokalųjį tinklą atskirtum nuo interneto ir sektum įdiegtų programų tinklinio aktyvumo, taip išaiškindamas ne tik šnipus, bet ir legalias programas, kurios bando patikrinti registracijos korektiškumą).

Jokie, net ir patys tobuliausi antivirusai nuo protingai sukonstruotų užkratų neapsaugos! Be to, jie kainuoja nemažus pinigus, dėl dažnų atnaujinimų suryja žymią tinklo srauto dalį, sistemoje sukelia konfliktus ir stabdo jos darbą, tuo tarpu OS su virusais gali susitvarkyti ir pati — jai nereikia jokių papildomų ramentų!

Išmėgink priėjimo kontrolę

Dabar aš kai ką tau pasakysiu, tačiau tik tuomet, jeigu pažadėsi, kad neužmėtysi manęs akmenimis. Priešingai nei, pavyzdžiui, BSD, Windows NT nėra daugiavartotojiška operacinė sistema, kadangi su kompiuteriu bet kuriuo metu gali dirbti tik vienas vartotojas, o prieš pradedant dirbti kito vartotojo vardu reikia užbaigti einamą sesiją (t.y. uždaryti visas programas ir atsiloginti), ir tik tada... O BSD sistemoje viskas paprasta: nuspaudei Alt–F#, t.y. persijungei į kaimyninę konsolę — ir viskas! Windows XP sistemoje galų gale atsirado galimybė keliems vartotojams su kompiuteriu dirbti vienu metu neužbaigiant savo sesijos (user switching funkcija), tačiau tarpusavio sąveikos tarp vartotojų mechanizmo kaip nebuvo, taip nėra.

Tiesa, einamoje sesijoje programas galima paleidinėti kito vartotojo vardu, tačiau tai, visų pirma, visiškai ne tas pats, o, antra, toli gražu ne visos programos sutinka su tokiu paleidimu, ir



dar mažiau jų tokiu atveju sugeba pilnavertiškai dirbti. Taigi be ritualinių apeigų būgno čia neapseisi. Jeigu neturi būgno, tiks ir paprasčiausias cinkuotas dubenėlis.

Atsispyrimo virusams idėjos esmė slypi teisingos priėjimo kontrolės politikos pasirinkime, tuomet antivirusas (arba bet kokia kita kenksminga programa) paprasčiausiai negalės pridaryti žymios žalos. Tam visas potencialiai pavojingas programas reikia paleidinėti savotiškoje smėlio dėžėje. Idealiu atveju tai būtų VMware tipo virtuali mašina, tačiau apie VMware mes jau ne kartą rašėme, o apie priėjimo kontrolę medžiagos praktiškai nėra.

Pradėsime nuo to, kad jokiu būdu nederėtų nuolat dirbti administratoriaus vardu, kadangi tuomet bet kokia paleista programa galės su sistema daryti viską, ką tik panorės. Administratoriaus vardu į sistemą jungtis reikia tuomet, kai atliekami „remonto" darbai: įdiegiamos naujos tvarkyklės, keičiami konfigūracijos parametrai ir t.t. Visą likusį laiką reiktų dirbti paprasčiausio vartotojo vardu su apribotomis teisėmis. Kuo mažiau pas jus privilegijų, tuo mažiau jų ir pas kiekvieną jūsų paleistą programą, tačiau daugelis programų atsisako veikti įprastinio vartotojo vardu, kadangi joms reikia rašyti į „Program Files" katalogą arba į kitas paprastiems mirtingiesiems draudžiamas vietas. Tuomet tenka garsiai mušti būgną ir užsiiminėti subtiliu konfigūravimu, tačiau po to... Po to ateina tyla bei ramybė — nei virusų, nei kokio kito malware.

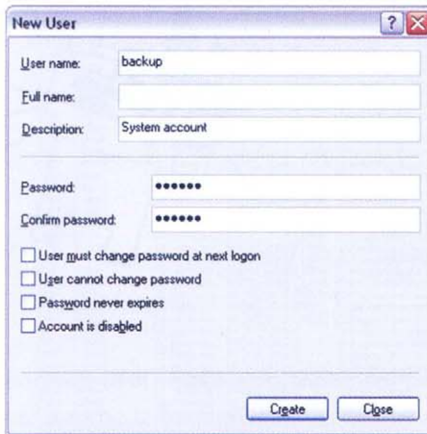
Savaime suprantama, periodiško rezervinio kopijavimo būtinybė egzistuoja iki šiol. Patikimiausia tai daryti į CD-R/RW, DVD-RW, ZIP, juostinius įrenginius ir kitus išorinius informacijos kaupiklius, bet tai nenašu, nepatogu, o ir šiaip kietųjų diskų patikimumas didesnis, nei to paties CD-RW. Pasielkime taip. Sukurkime naują vartotoją su administratoriaus teisėmis: Start -> Control Panel -> User Accounts -> Add -> User Name tegu būna „backup" -> Other -> Administrators. Tuomet užeikime naujo vartotojo vardu į sistemą, sukurkime katalogą „general-store" (t.y. bendra saugykla) ir į jį nukopijuokime viską, kas mums būtina ir reikalinga. Tada ant šio katalogo pavadinimo spaudžiam dešinį pelės klavišą, atsiradusiame kontekstiniame meniu išsirenkame Properties, o ten — Security, t.y. patenkame į prie šio katalogo prieinančių vartotojų sąrašą. Pagal nutylėjimą šis katalogas prieinamas visiems, kas jokiu būdu nesiderina su mūsų planais, todėl iš pradžių nuspaudžiame Security tabe esantį mygtuką Advanced ir ten nuimame varnelę „Inherit from parent the permission entries that apply to child objects", atsidariusiame dialoge pasirenkame Copy, o tada pašaliname visus vartotojus, išskyrus šį katalogą sukūrusį vartotoją, t.y. „backup". Viskas!!! Dabar šis katalogas neprieinamas niekam, net ir sistemai! Ir tik jo savininkas gali įeiti į Security skiltį ir visus sugrąžinti į savo vietas. Dėmesio! Administratorius to negalės padaryti! (o tiksliau, galės, tačiau iš pradžių turės perimti nuosavybę (ownership) į šį katalogą). Gera apsauga nuo virusų ir kitokių destruktyvių programų, tiesa? Beje, o kas nutiktų, jeigu atsitiktinai (specialiai) pašalintume vartotoją „backup"? Juk tuomet prie archyvo niekas negalės prieiti! Laimė, į operacinės sistemos sudėtį įeinantis įrankis chkdsk atpažįsta tokią situaciją ir, suradus atitinkamą katalogą-zombį, visas teises automatiškai sugrąžina į savo vietas, taip prikeldamas informaciją iš nebūties.

Smėlio dėžė — ne tik vaikų džiaugsmas

Mūsų kita užduotis bus sukurti „smėlio dėžę" visoms toms programoms, kurios gali būti atakuotos iš interneto, prie kurių galima priskirti IE, FireFox, Outlook Express, The Bat, ICQ ir kitas. Kiekviena jų turi būti paleista vartotojo su apribotomis teisėmis vardu, kuris neturi priėjimo prie jokių katalogų, išskyrus tuos, kurie akivaizdžiai reikalingi pačiai programai. Iš esmės visoms tokioms programoms galima sukurti vieną vartotoją su apribotomis teisėmis, kurį galima pavadinti, pavyzdžiui, „sandbox" (t.y. smėlio dėžė), tačiau šiuo atveju per IE įsibrovęs kirminas galės sugadinti per daug metų sukauptą pašto bazę, kas būtų skaudu. Taigi geriausia kiekvienai programai sukurti po atskirą vartotoją (žinoma, tai padidina sistemos reiklumą resursams, tačiau ne taip radikaliai, kad tai iš esmės jaustųsi)

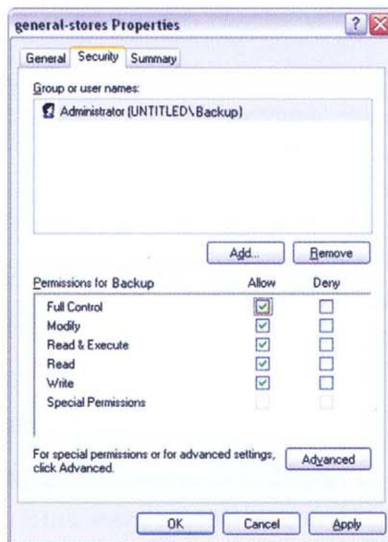
Taigi sukuriame vartotoją su apribotomis teisėmis „sandbox", kiekvieno katalogo arba ištiso disko apskritai, į kurį norime uždrausti prieiti šiam vartotojui, saugumo savybėse jį pridedame ir aiškiai uždraudžiame jam priėjimą, t.y. suteikiame Deny teisę, kuri draudimo politikoje visada yra viršesnės už Allow teises, todėl iš sąrašo pašalinti visus vartotojus visiškai nebūtina, tačiau Deny teisę patariama naudoti atsargiai. Užbaigus šią paprastą procedūrą sandbox'ui liks tik tie katalogai, kurie jam reikalingi. Dažniausiai tai pačios programos katalogai, kuriuose, beje, reikėtų uždrausti rašymo į vykdomas bylas ir bibliotekas teises.

Pamėginkime tokioje smėlio dėžėje paleisti, pavyzdžiui, FireFox. Sukuriame nuorodą (shortcut) su firefox.exe (jeigu tik to už mus nepadarė įdiegiklis), spaudžiam ant jos dešinį pelės klavišą, einam į Properties, tada — Advanced ir ten uždedame varnelę „Run with different credentials", spaudžiam OK ir paleidžiam. Prieš mūsų akis pasirodo



› Dabar prieiti prie katalogo gali tik vartotojas „backup". Du pelės paspaudimai – ir jokių virusų

grėsmingas dialogas, kuriame reikalaujama įvesti vartotojo vardą ir slaptažodį. Įvedame ir... Ugninė Lapė nepasileidžia! Beje, Linux/BSD sistemose tokia operacija atliekama be jokių nesklandumų. O mums vėl reikės mušti būgną arba, konkrečiau šnekant, pasinaudoti Marko Rusinovičiaus bylų monitoriumi, kuris parodo, kokias būtent failines operacijas atliekant programa patiria nesėkmę (štai kaip gamintojai reaguoja į klaidų pranešimus). Pradžiai parsisiunčiame bylų monitorių: www.sysinternals.com/Utilities/Filemon.html. Beje, jis užima mažiau nei du šimtus kilobaitų ir platinamas visiškai nemokamai! Paleidžiame jį administratoriaus vardu, sukuriame nuorodą ir uždedame mums jau pažįstamą varnelę „Run with..."! Šiuo atveju bylų monitorius pasileidžia, kadangi jis suprogramuotas tvarkingai, ir mes greitu sportiniu žingsniu einame į Options -> Filter/Highlight arba spaudžiam <Ctrl-L>. Atsiradusiame dialogo lange uždedame visas varneles, išskyrus „Log Successes", kadangi mums nėra ko loginti sėkmingai atliktas operacijas — mums reikia klaidų! Spaudžiam OK ir perleidžiam programą (filtras pradės veikti tik po perleidimo). Vėl paleidžiam Ugninę Lapę. Ką gi mes matom? Iš pradžių — dinaminių bibliotekų paieškos tuose kataloguose, kur



› Prieiti prie katalogo gali tik specialiai sukurtas vartotojas „backup"

jų nėra, klaidos (tai normalu), o toliau FireFox tiesiog WINNT kataloge bando sukurti katalogą Mozilla (čia FF saugo savo nustatymus, puslapių cache ir t.t.), kur jos, savaime suprantama, neleidžia ir ji tyliai numiršta.

Taip... Čia tai bent užduotis. Išbandome komandinės eilutės įrankį runas, su kuriuo darome taip: „runas /user:sandbox firefox.exe" (šiuo atveju firefox.exe turi būti einamam kataloge, priešingu atveju reikia nurodyti pilną kelią iki vykdomos bylos). Mūsų dalykiškai paklausia slaptažodžio ir... nieko! Dabar FireFox lenda į „Documents and Setting\Default User", kur jis taip pat neturi jokių teisių! Ką daryti?! Kame reikalas?! Pasirodo, tame, jog korektiškam daugelio programų veikimui dar būtina užkrauti ir vartotojo, kurio vardu mes ją paleidžiam, profilį, todėl teisingas variantas atrodo taip: „runas /profile /user:sandbox firefox.exe". Dabar naršyklė pasileidžia sklandžiai!

Tuo tarpu Opera savo cache saugo ne vartotojo profilyje, o tiesiog savo kataloge (beje, tai priklauso nuo naršyklės nustatymų), todėl vartotojui sandbox reikia suteikti teises rašyti į katalogą „program files\opera".

Su likusiomis programomis viskas atliekama analogiškai. Jeigu nepadeda bylų monitorius, tuomet parsisiunčiam sisteminio registro monitorių (www.sysinternals.com/Utilities/Regmon.html) ir žiūrim, kurių šakų programai reikia. Mažas povandeninis akmuo: deja, klaviatūros įvedimo negalima nukreipti į bylą, todėl slaptažodį tenka įvedinėti kiekvieną kartą, kas užknisa. Beje, programuotojai paprasčiausiai parašo programą, kuri neturi tokių trūkumų. O mums svarbiausia — sukurti krūvą vartotojų ir taip paskirstyti priėjimo teises, kad kenksmingos programos neturėtų jokių šansų nei daugintis, nei šnipinėti.

Pabaiga

Apsaugotos sistemos sukūrimas be antivirusų — tai realu! Tegu iš pradžių mums reikės nudirbti daug darbo ir smarkiai pasukti galvą, sukuriant tiek vartotojų, kad būtų galima pilnai izoliuoti vieną potencialiai pavojingą programą nuo kitų, tačiau po to tu tikrai žinosi, kad, dirbdami su tavo mylima mašina, namiškiai su ja negalės padaryti nieko blogo.

INFO

› Jeigu katalogo arba bylos savybėse tu netyčia nerasi Security skilties, dėl visko gali kaltinti vaikinus iš „Microsoft". Jie nusprendė viską taip supaprastinti, kad pagal nutylėjimą saugumo konfigūravimo galimybės nuo vartotojų yra paslėptos. Sugrąžinti viską į savo vietas galima taip: Start –> Run –> explorer.exe –> Tools –> Folder options –> View –> nuimk varnelę nuo „Use simple file sharing".

› „Internet Explorer" ir saugus pasaulinio voratinklio naršymas

Kai kurie protingi žmonės jau seniai susidūrė su Internet Explorer naršyklės saugumo problema — šiems žmonėms iškilo klausimas, kaip galima būtų saugiai dirbti su šia į Windows sistemas įmontuota naršykle. Miklios gudrių programuotojų rankos sukūrė įrankį, kuris vadinasi DropMyRights. Plačiau apie jo galimybes bei naudojimą gali paskaityti čia: http://msdn2.microsoft.com/en-us/library/ms972827.aspx, o parsisiųsti iš čia: http://download.microsoft.com/download/f/2/e/f2e49491-efde-4bca-9057-adc89c476ed4/dropmyrights.msi

TINKLINIS KAMUFLIAŽAS

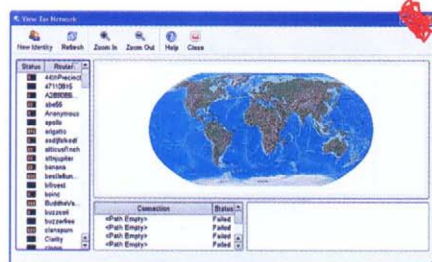
IŠMOKYTI KARČIOS PATIRTIES, HAKERIAI NAUDOJA VPN SUSIJUNGIMUS. TAI TIKRAS ATRADIMAS: IR TINKO SRAUTĄ NEPERTRAUKIAMAI ŠIFRUOJA, IR ANONIMIŠKUMĄ GARANTUOJA. BENT JAU TAIP TVIRTINA TIE, KAS TEIKIA ŠIAS PASLAUGAS. IŠ TIESŲ VISKAS GALI BŪTI KIEK KITAIP: STAIGA SERVERYJE IŠ NIEKUR GALI ATSIRASTI ĮSPŪDINGO DYDŽIO LOGAI, O PO TO IŠ VISO GALI PAAIŠKĖTI, KAD ŠIAS PASLAUGAS KONTROLIUOJA KOMPETENTINGI ORGANAI. IR KAIP AŠ APSIDŽIAUGČIAU, JEIGU TAI BŪTŲ TIK MANO LIGUISTOS VAIZDUOTĖS VAISIUS. TOLI GRAŽU — TAI REALAUS GYVENIMO PAVYZDYS! PO TOKIŲ INCIDENTŲ PRADEDI MĄSTYTI APIE TO PATIES VPN ALTERNATYVĄ.

NESTANDARTINIAI ANONIMIŠKUMO IŠSAUGOJIMO METODAI

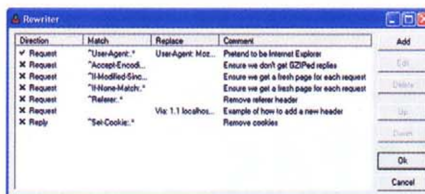


Privati simbiozė

Kai pradedama kalbėti apie VPN alternatyvą, tuomet pirmas į galvą atėjęs dalykas, ko gero, būna SSH tuneliavimas. Beje, tai labai geras daiktas, jį paprasta eksploatuoti, tačiau tokiu atveju reikia įdėti šiek tiek pastangų ir minimalių investicijų. Mūsų žurnalo puslapiuose mes daug kartų pasakojome apie šio būdo įgyvendinimą, todėl nesikartosime. O štai šiandien mes aptarsim du visiškai kitokius metodus, kurie absoliučiai nepanašūs į tai, ką naudojome anksčiau. Pirmasis jų remiasi iš karto dviejų įrankių (Tor ir Privoxy) panaudojimu. Pirmąjį mes



› Nodų sąrašas ir paketų kelionės maršrutas pasaulio žemėlapyje



› Su tokiu konstruktoriumi galima sukonfigūruoti automatinį bet kokių HTTP užklausos parametrų pakeitimą

panaudosime kaip tinklo srauto šifravimo ir anonimiškumo išsaugojimo priemonę, o antrąjį — kaip galingą HTTP(S) protokolais perduodamų duomenų filtravimo įrankį, kuris skrupulingai šalins visą tavo klientinių programų perduodamą kompromituojančią informaciją.

Pasakyti, kad Tor — tai nepaprasta programa, reiškia nieko nepasakyti. Patikėk, tai tikrai unikalus daiktas. Anonimiškumo užtikrinimo principas remiasi paskirstyta serverių, kitaip dar vadinamų nodais, tarp kurių duomenys perduodami šifruotu pavidalu, sistema. Susijungimui paprastai naudojami trys serveriai, kurie suformuoja laikiną grandinę. Kiekvienas serveris parenkamas atsitiktiniu būdu, tuo pačiu jis žino tik tai, iš kurio mazgo (iš kurios grandies) gavo duomenis ir kam jie skirti. Net ir kuriame nors viename serveryje perėmus duomenis susekti pilną paketų maršrutą (o tuo pačiu ir jų siuntėją) neįmanoma. Tačiau tai dar ne viskas. Prieš išsiuntimą paketas nuosekliai užšifruojamas su trimis raktais: iš pradžių trečiam mazgui skirtu raktu, po to antram, ir galų gale pirmam mazgui skirtu raktu. Kai pirmasis mazgas gauna paketą, jis dešifruoja „viršutinį" šifro sluoksnį ir sužino, kur toliau siųsti paketą. Antrasis ir trečiasis serveris elgiasi analogiškai.

Vos tik grandinė suformuota, galima pradėti duomenų perdavimą. Kad sistema nepatirtų greičio nuostolių, viena grandinė naudojama 10 minučių eigoje, ir tik po šio periodo grandinė performuojama iš naujo. Dabar apie tai, ką galima paleisti per šį tunelį. Tor dirba tik su TCP srautais ir jį galima panaudoti su bet kokia programa, kuri veikia per SOCKS. Tuo atveju, kai programoje negalima akivaizdžiai nurodyti proxy serverio, praverčia soksifikatoriai, pavyzdžiui, SocksCap (www.socks.permeo.com), FreeCap (www.freecap.ru) arba tvarkyklės lygyje veikiantis Permeo Premium Agent (www.permeo.com/products/premium_agent.html).

Tokį gudrų duomenų perdavimo būdą sukūrė programuotojai pagal federalinį JAV karinių pajėgų užsakymą. Ilgai sistema nebuvo laisvai platinama ir ją naudojo tik ribotas vyriausybinių organizacijų bei tarnybų ratelis. Tuo o dabar Tor'o grožybėmis gali pasinaudoti ir tu — nepraleisk tokios galimybės.

Dabar pakalbėsim apie Privoxy. Iš esmės tai paprasčiausias HTTP proxy, kuriame apstu žvėriškai galingų tinklo srauto filtravimo funkcijų, naudojamų užtikrinti vartotojo anonimiškumui, pakeisti dinaminių web puslapių turiniui, valdyti cookies, apriboti priėjimą prie tam tikrų svetainių bei pašalinti reklamas, reklamines antraštes, iššokančius langus ir spyware. Bet kokie filtravimo veiksmai gali būti aiškiai užprogramuoti su vidine taisyklių sistema. Mums svarbu tai, kad Privoxy analizuoja HTTP antraštes ir, jei būtina, jas pakeičia pagal sukonfigūruotą taisyklių rinkinį, kuris užkerta kelią bet kokios antraštėse esančios kompromituojančios informacijos perdavimui. Taip pat užkertamas kelias ir vartotojo sesijos užfiksavimui, pagal kurią jį būtų galima identifikuoti tarp daugelio kitų klientų.

Rengiamės kamufliažą

Anksčiau, kada Tor tik atsirado, tekdavo ilgai ir nuobodžiai kapstytis po tekstinius Privoxy ir Tor konfigus. Dabar viskas kur kas paprasčiau: oficialioje Tor svetainėje (http://tor.eff.org/index.html) galima gauti paruoštą paketą, kuris susideda iš paties Tor, Privoxy bei grafinės visos sistemos valdymo aplinkos Vidalia. Įdiegimo metu iš viso nereikia nieko judinti: viskas bus įdiegta ir be tavo pagalbos. Pasibaigus šiam procesui neskubėk ieškoti Tor nuorodos ir jos paleidinėti. Kadangi mes įdiegėme programos valdymui skirtą GUI aplinką, paleisti reikia būtent ją. Sisteminiame lauke (system tray) atsiras žalias perbrauktas svogūnas. Tai reiškia, kad servisas atjungtas. Spustelėk ant šios ikonėlės deši-

INFO

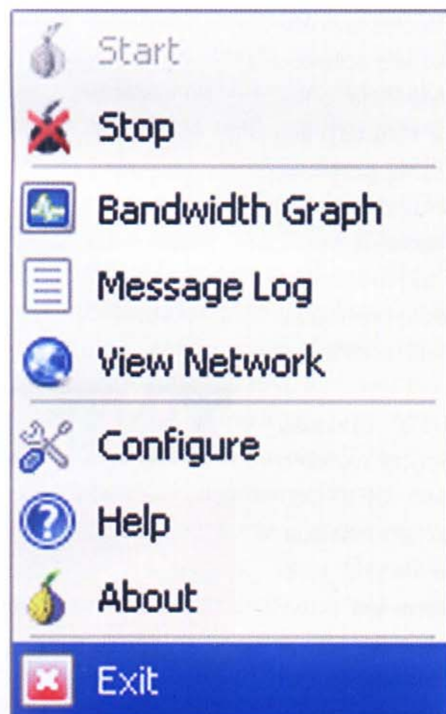
› Tau iškilo klausimas, kokia sistema geriausiai tinka anonimiškumo išlaikymui? Atsakau: Anonym OS (http://sourceforge.net/projects/anonym-os/). Ši operacinė sistema sukurta remiantis OpenBSD ir iš karto sukonfigūruota skaidriai šifruoti tinklo srautą bei išsaugoti anonimiškumą, taip pat įdarbinant ir Tor priemones. Kitos anonimiškam naršymui skirtos OS: ELE (www.northernsecurity.net/download/ele/), Virtual Privacy Machine (wiki.noreply.org/noreply/VirtualPrivacyMachine), Phantomix (http://phantomix.ytternhagen.de/).



› http://tor.eff.org/ — oficiali Tor svetainė.
www.privoxy.org — Privoxy puslapis.
www.vidalia-project.net — patogi GUI sąsaja, skirta Tor valdymui.
http://privacy.hro.org — svetainė apie privatumą ir asmeninio gyvenimo nepriklausomybę tinkle.

nį pelės klavišą, ir atsiradusiame meniu pasirink Start. Po to programa pradės lįsti į internetą (dėl ko greičiausiai ims žviegti ugniasienė), kad galėtų parsisiųsti naujausią nodų sąrašą. Iš esmės dirbti galima jau dabar — Tor pagal nutylėjimą veikia kaip TCP proxy serveris (per 9050 jungtį), t.y. jį galima įrašyti naršyklėje ir taip patikrinti jo kovines galimybes, tačiau skubėti neverta.

Jeigu programa nedirba su socks4a protokolu, o vietoje proxy serverio tiesiogiai nurodytas tavo Tor klientas (pagal nutylėjimą IP 127.0.0.1, 9050 jungtis), tuomet tokia programa bando savarankiškai nustatyti užklausiamo serverio IP adresą. Greičiausiai tokiu atveju ji pasiųs užklausą į tavo tikro interneto paslaugos tiekėjo DNS serverį. Maža to, kad taip tu išsiduosi tiekėjui, tai dar ir nutolusiam serveriui parodys tavo naudojamą DNS (kuris greičiausiai yra tiekėjo potinklyje). Patikrinti tokios baigties galimybes nesudėtinga, jeigu per proxy užeitum į www.dnsstuff.com/tools/aboutyou.ch svetainę, kur pamatytum savo DNS serverio adresą. Tačiau ne veltui mes įdiegėme Privoxy — būtent jis mums padės išvengti panašios baigties, juo labiau, kad šis stebuklingas proxy nuo pradžių kurtas darbui su Tor'u, todėl tau neteks aiškintis gudrių jo taisyklių ir konfigūracijos. Pakanka jį tiesiog paleisti.



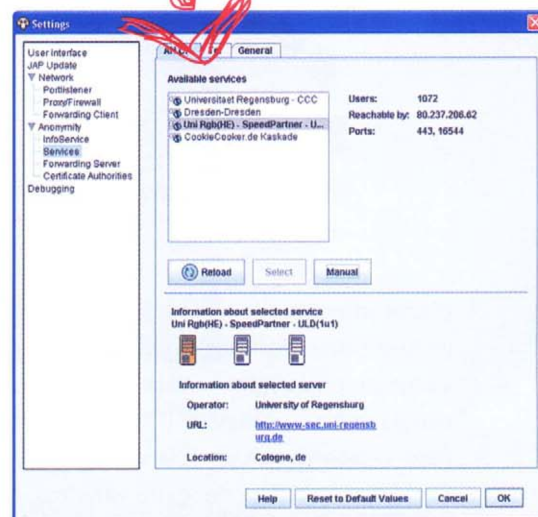
› Tor valdymui skirtos GUI aplinkos meniu

Po to per 8118 jungtį pradės veikti proxy, kuris draus tai, kas gali tave išduoti, ir toliau viską nukreipinės Tor'ui. Siekiant didesnio patogumo rekomenduoju įdiegti Firefox įskiepį — TorButton (www.freehaven.net/~squires/torbutton/). Dabar įjungti ir išjungti Tor'ą tu galėsi vienu pelės klavišo paspaudimu. Egzistuoja net specialus TorPark rinkinys (http://freehaven.net/~arrakis/torpark.html), susidedantis iš Firefox ir Tor, kurį galima paleisti iš flash atminties kortelės. Patikrinti sistemos veikimą nesudėtinga: pakanka užeiti į www.ip2location.com svetainę ir pažiūrėti, kokią informaciją ji pateikia apie tavo buvimo vietą. Patikėk, savo tikrojo IP adreso ir interneto tiekėjo pavadinimo tu ten nepamatysi, kaip kad nepamatysi ir užuominų apie proxy, kadangi susijungimo antraštėse nėra visų tai parodančių aplinkos kintamųjų:

HTTP_FORWARDED: (none)

HTTP_X_FORWARDED_FOR: (none)

Programa Vidalia pateikia keletą kitų įdomių galimybių. Su Bandwidth Graph tu gali stebėti sistemos tinklinį aktyvumą. Message Log langelyje rasi informaciją apie Tor veiklą ir iškilusias klaidas. Sezono topas — punktas View Network, kuriame atvaizduojama informacija apie sistemos nodus, o žemėlapyje grafiškai atvaizduojamas tavo paketų judėjimas. Apskritai dirbant tokia sistema tau suteikia daugybę privalumų. Be pastovaus susijungimo šifravimo tu gauni visada veikiantį anonimizuoklį. Daugiau nereikia ieškoti proxy ir socks serverių, kurie tau nežinant gali viską loginti ir, be viso kito, dvesia kaip musės. Tiesa, iškyla klausimas: ką daryti, jeigu prireikia laikytis pastovios buvimo vietos? Pavyzdžiui, vykdant piktadarystes su mokėjimais arba lankant resursus, kurie savo tinklo srautą leidžia siųsti tik tam tikros šalies vartotojams. Tam konfigūracinėje Tor byloje (torrc) galima panaudoti specialią direktyvą „StrictExitNodes 1", kuri reiškia, jog išėjimo taške bus naudojami griežtai apibrėžti nodai. Pačius nodus galima sukonfigūruoti su direktyva exitnodes: exitnodes nodo_pavadinimas1, nodo_ pavadinimas2 ir t.t. Kad šito nereikėtų daryti rankiniu būdu, vienas iš Tor programuotojų sugalvojo sukurį įrankį Nodeblock (http://sandos.ath.cx/~badger/nodeblock.html), kuris savarankiškai parenka naudojamų Onion maršrutizatorių (kitas nodų pavadinimas) sąrašą pagal geografinę buvimo vietą.



› Nulinis anonimiškumo lygis — būtina pasirinkti serverį

Anonimiškumas vokiškai

Viename vokiečių institutų buvo sukurtas gana gudrus anonimiškumo išsaugojimo būdas. Į vartotojo sistemą įdie-



giama speciali proxy programa JAP (http://anon.inf.tu-dresden.de/index_en.html), kuri perima visas vartotojo prisijungimo užklausas, jas užšifruoja ir saugiu režimu išsiunčia į specialų tarpinį serverį (taip vadinamą miksą). Čia esmė tame, kad miksą vienu metu naudoja daugybė vartotojų, o pati sistema sukurta taip, kad kiekvienas iš jų serveriui būtų visiškai vienodas. Kadangi visi klientai vienodi, tai ir aptikti vieną konkretų vartotoją nėra įmanoma. Miksai paprastai įdiegiami geranoriškais tikslais, pagrinde universitetuose, ir jie oficialiai tvirtina, kad neregistruoja jokių logų.

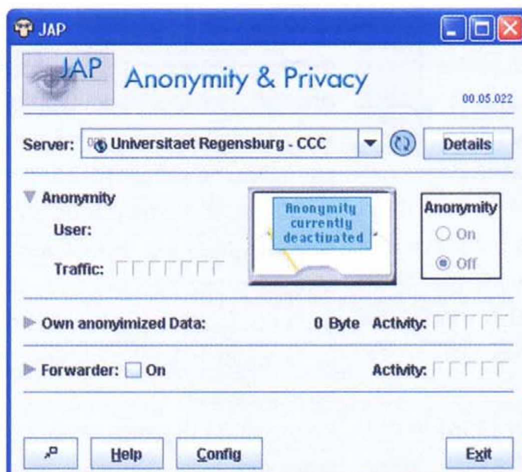
Vartotojo dalyvavimas sistemos konfigūravime minimalus — iš esmės, jam reikia įdiegti JAP proxy ir pasirinkti teisingą miksą. Straipsnio rašymo metu programoje buvo prieinami 5 anonimiški serveriai. Kiekvienam jų išvedama skirtinga vienu metu esančių vartotojų informacija. Pasirinkimas paprastai nevienareikšmiškas: kadangi kuo daugiau vartotojų, tuo daugiau anonimiškumo, tačiau tuo mažesnis susijungimo greitis (serverio resursai nėra neriboti). Kita vertus, didesnį greitį galima gauti pasirinkus ne tokį populiarų servisą, tačiau taip prarandamas aukščiausias galimas saugumo lygis. Beje, anonimiškumo lygis atvaizduojamas specialioje skalėje.

Ypač įdomu tai, kad šie serveriai visiškai suderinami su Tor'o nodais. Su pačia programa parsisiuntus tarpinių serverių sąrašą, juos galima drąsiai naudoti. Beje, tu turi teisę pats pasirinkti, iš kokio nodų kiekio formuoti grandines, kaip dažnai jas keisti ir t.t. Pagal nutylėjimą servisas susijungimus priima per 4001 jungtį, todėl nepamiršk naršyklėje vietoje naudojamo proxy serverio įrašyti 127.0.0.1:4001.

Organizuojam maskaradą

Kiekvieno web puslapio apsilankymo metu tavo naršyklė perduoda masę techninės informacijos. Tokie tave kompromituojantys duomenys, kaip OS lokalizacija, naršyklės versija, laiko juosta, puslapis, iš kurio buvo pereita, perduodami taip vadinamuose aplinkos kintamuosiuose. Juos galima lengvai peržiūrėti apsilankius www.showmyip.com svetainėje. Čia visa informacija pateikiama kaip ant delno. Užsimaskuoti amerikiečio pavidalu lengva — pakanka įdiegti anglišką langinių versiją ir pasirinkti teisingą laiko juostą. Tačiau kitais atvejais rasti tinkamą distributyvą bus gana problematiška. Ir šiaip, visur ir nuolat sutinkamos situacijos, kada reikia pakeisti kitų aplinkos kintamųjų reikšmes. Tuomet ir iškyla idėja: o ką, jeigu mes panaudotume tam tikrą filtrą tarp tinklo ir kliento, kuris galėtų pagal mūsų poreikius pakeisti HTTP antraštes, taip suklaidindamas bet kurį adminą? Čia mums padės Odysseus (www.wastelands.gen.nz/odysseus/) — tai tinklo paketas, kuris pirmą kartą buvo pademonstruotas hakerių konferencijoje Defcon ir kurį sukūrė tikri savo reikalo žinovai.

Ši programa — tai galingas HTTP užklausų konstruktorius, suteikiantis galimybę veikimo metu (on–the–fly) keisti sausainukus, GET/POST užklausas, įtraukti papildomus parametrus, žodžiu, be ribų valdyti daugybę dalykų. Kaip ir ankstesnės programos, Odysseus yra proxy serveris, kuris pagal nutylėjimą veikia per 50000 jungtį. Iš esmės analogiškus veiksmus galima atlikti ir su aukščiau aprašytu Privoxy, tačiau Odysseus atveju viskas kur kas paprasčiau. Čia



> Pasirenkame dėmesio vertą serverį su dideliu vartotojų kiekiu — tai padidins galimybę išlikti anonimiškam

DANGER!

> Naudodamasis Tor, tu jokiu būdu savo kompiuterio neįtrauki į tų serverių, kurie naudojami anonimiškumui užtikrinti, sąrašus. Tai daroma savanoriškai ir laisva valia, todėl jeigu tik nori, perskaityk specialią tam skirtą dokumentaciją: http://tor.eff.org/docs/tor-doc-server.html.en.

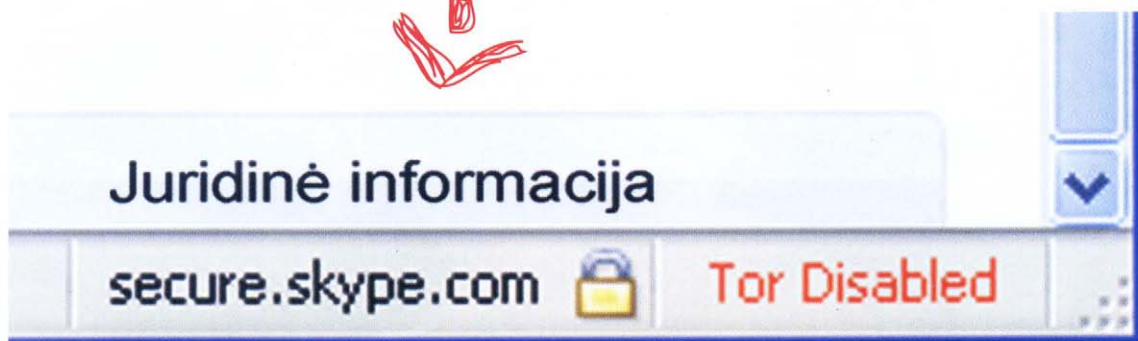
> Anonimiškumas — tai tavo paties saugumo užstatas, o ne pretekstas įstatymams prieštaraujančiai veiklai.

INFO

> Panaudojant Tor ir Tor–DNS (http://sandos.ath.cx/~badger/tordns.html) galima sukurti neblogą bazę none–abuse hostingui. Pagal nutylėjimą tavo svetainė bus išsprendžiama kaip .onion zonos domenas.







› Tor įjungti/išjungti geriausia su papildomais įrankiais. Firefox naršyklės atveju tai padės padaryti TorButton

visi veiksmai atliekami patogioje ir malonioje GUI aplinkoje, todėl atkrenta bet kokia būtinybė terliotis su taisyklių ir filtrų sintakse, kaip kad buvo Privoxy atveju. Ir tai yra kieta. Tarkim, tau reikia pakeisti User Agent (informaciją apie naudojamą naršyklę). Tam spustelėk dešinį pelės klavišą ant sisteminiame lauke matomos programos ikonėlės, o tada pasirink įrankį Rewriter (automatinio serveriui perduodamų parametrų pakeitimo priemonė). Atsidariusiame lange pateikiamas naudojamų taisyklių sąrašas: pasirenkame ^User–Agent ir žiūrim į taisyklės savybes. Principas paprastas: Odisėjus perduodamoje užklausoje ieško Match lauke nurodyto parametro ir pakeičia jį Replace lauke įrašyta eilute. Taigi iš tavęs reikalaujama tik į reikiamus laukus įrašyti atitinkamas reikšmes. Pavyzdžiui, norint apsimesti vartotoju su Internet Explorer, pakanka į Replace lauką įrašyti eilutę „User–Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)". Analogiškai galima filtruoti sausainukus (pavyzdžiui, savo servise siekiant realizuoti gudrią autentifikaciją, kuri analizuotų būtent šį parametrą) ir t.t.

Bet kokios nutolusiam serveriui siunčiamos užklausos perimamos, o užklausoje perduodami kintamųjų duomenys lengvai koreguojami, jeigu Odisėjuje aktyvuotas Interceptor režimas. Jis aktyvuojamas analogiškai per išplaukiantį meniu, kurį gausi ant sisteminiame lauke esančios programos ikonėlės paspaudęs dešinį pelės klavišą. Po to pabandyk užeiti į kokią nors svetainę. Tuojau pat pasirodo langas su visais parametrais, kiekvieną kurių lengva pataisyti. Išstudijuok, pataisyk, ką reikia, ir spausk Done — dabar visi parametrai (taip pat ir ištaisytieji) bus perduoti tikram serveriui.

Su Activity Log galima tiksliai išanalizuoti naršyklės ir nutolusio serverio bendravimą — tai dar vienas programos darbo režimas. Beje, kiekvienam režimui galima priskirti karštąjį klavišą ir tada greitai jį iškviesti. Tai ir dar daug kitų dalykų galima sukonfigūruoti derinant programos opcijas. Ši programa iš tiesų galinga, todėl siekiant užtikrinti saugumą tokio įrankio negalima neįvertinti. Labai dažnai tenka pakeisti naudojamos naršyklės tipą (su User Agent), pašalinti Referer. Man net tekdavo į užklausą pridėti X–Forwarder, Via ir Proxy–connect laukus, kad taip priversčiau serverį galvoti, jog aš dirbu per viešą proxy serverį (oficialų, su logais, ir dėl to nekeliantį įtarimų).



› Odisėjaus logas: naršyklės bendravimas su serveriu kaip ant delno



Kaip grūdinosi „America Online"

STAMBIAUSIO TIEKĖJO PAKILIMŲ IR NUOPUOLIŲ ISTORIJA

„AMERICA ONLINE" — VIENAS STAMBIAUSIŲ IR SĖKMINGIAUSIŲ TIEKĖJŲ ISTORIJOJE. GERIAUSIAIS LAIKAIS AOL PASLAUGOMIS NAUDOJOSI DAUGIAU NEI 32 MILIJONAI ABONENTŲ IŠ JAV, KANADOS, PRANCŪZIJOS, VOKIETIJOS, JAPONIJOS IR LOTYNŲ AMERIKOS. 90–ŲJŲ VIDURYJE DAUGELIUI ŽMONIŲ INTERNETAS ASOCIJAVOSI SU AOL PREKINIU ŽENKLU. TAČIAU BĖGANT METAMS SITUACIJA KEITĖSI, O AOL ATVEJU JI KEITĖSI NE Į GERĄJĄ PUSĘ. AOL PRIĖMĖ DAUGYBĘ NETEISINGŲ SPRENDIMŲ, O 2006 METAIS AMERIKOS ŽURNALAS PCWORLD JĄ PRIPAŽINO BLOGIAUSIU VISŲ LAIKŲ IR TAUTŲ TIEKĖJU. KAS GI YRA TA „BLOGIO IMPERIJA", KAIP JĄ PRAMINĖ KOMPIUTERISTAI? PABANDYKIM IŠSIAIŠKINTI.

Prekinio ženklo gimimas

„America Online" (arba tiesiog AOL) savo veiklą pradėjo 80–ųjų pradžioje kaip mažytė ir abejotina firma, kuri vadinosi „Control Video Corporation" (CVC), o jos savininkas buvo Viljamas von Meisteris. Šiai kontorai priklausė Atari 2600 vartotojams skirta online paslauga Gameline. Meisteris sugalvojo naujovišką sistemą: kaip remiantis duomenų perdavimo per modemą technologija užkalti neblogus pinigus. Iš pradžių jis planavo sukurti muzikinę paslaugą, tačiau kompanijai „Warner Brothers" ši idėja nelabai patiko, todėl Viljamui jos teko atsisakyti. Taip jis apsistojo ties žaidimais. Meisteris sukūrė ir išleido keistą Atari 2600 skirtą įrenginį, išoriškai atrodžiusį kaip įprastinis kartridžas, kurio viduje buvo modemas. Paslaugos veikimo principas buvo paprastas: priedas per modemą susisiekdavo su centriniu CVC serveriu, iš kur vartotojas galėjo parsisiųsti bet kokius jam patikusius žaidimus (savaime suprantama, ne už dyką). Žaidimai vidutiniškai pasileisdavo 5–10 kartų, po ko vartotojas vėl turėdavo užeiti į CVC ir įnešti eilinę pinigų sumą. Sistema suteikdavo galimybę saugoti rekordų



AOL boikotavimas


„America Online“ logotipas iki 2004 metų


Dabartinis AOL logo

lentelę, o Gameline netgi organizuodavo kažką panašaus į čempionatus.

1983 metais firma atsidūrė prie bankroto ribos. „Control Video“ investuotojas Frenkas Kaufildas nusprendė į verslą įtraukti naujų žmonių ir taip ištaisyti susiklosčiusią situaciją. Jis kreipėsi į savo draugą Džimą Kimsį, kuris greitai pradėjo dirbti kaip gamybos konsultantas. Tuo pat metu kaip pardavimų specialistas prie CVC prisijungė Styvas Keisas. Keletą metų kompanijoje vyko įvairūs pertvarkymai: kadrų, ideologiniai ir t.t. Viskas baigėsi tuo, kad firma buvo pervadinta į „Quantum Computer Services“, o paslaugos įkūrėjas misteris von Meisteris tiesiog pabėgo nuo sunkumų. Nuo to laiko apie jį nieko nežinoma.

1985 metais Kimsis, kuris nematė akivaizdaus pagerėjimo, nusprendė visiškai pakeisti kompanijos strategiją. Būsimoji AOL dabar orientavosi į tuos žmones, kurie nelabai susigaudė kompiuteriuose, ir vietoje įprastinės programos–terminalo pradėjo naudoti tik savo pačios programinę įrangą. Komandinę eilutę pakeitusi grafinė sąsaja smarkiai palengvindavo žmonių bendravimą su kompiuteriu.

Kompanija pradėjo teikti visiškai naujas paslaugas: mokamą priėjimą prie stambių jungtinių BBS, skirtų Commodore 64 ir 128 kompiuteriams (šis elektroninis tinklas buvo pavadintas Quantum Link arba tiesiog Q–Link).

1988 metais į Styvą Keisą kreipėsi kompanijos „Apple“ atstovai, kurie jam pasiūlė sukurti į Q–Link panašią paslaugą, kuri būtų skirta Apple II ir Macintosh kompiuteriams. Šis pasiūlymą priėmė ir greitai pasaulio šviesą išvydo sistema, pavadinta AppleLink Personal Edition. Vartotojai liko nepatenkinti tokiu paslaugos pasikeitimu: anksčiau egzistavusi AppleLink jiems patiko labiau, kadangi, jų nuomone, AL PE nesuteikdavo priėjimo prie „tikrojo“ AppleLink'o. Greitai naujosios paslaugos teikimas buvo nutrauktas.



Retas kolekcinis AOL diskas



Nepaisant nesėkmės su Apple, Quantum'e toli gražu niekas nesiruošė atsipalaiduoti, todėl 1988 metų rugpjūtį buvo sukurtas AK teikiamos paslaugos analogas PCLink, o 90–ųjų pradžioje paslaugos pradėtos teikti DOS ir Windows vartotojams. Oficialiai Quantum Computer Services pavadinimas į America Online buvo pakeistas 1991 metų spalio mėnesį.

Būtent tuo metu AOL pradėjo teikti daugybę naujų online interaktyvių paslaugų, tarp kurių buvo pačios įvairiausios pokalbių svetainės ir konferencijos, online žaidimai ir kiti dalykėliai. Daugelis žaidimų rėmėsi grafine chat sistema, o AOL tapo šios srities naujakure. Ankstyvieji kompanijos vartotojai greičiausiai pamena tokius pavadinimus, kaip Habitat ir Club Caribe. Manau, jog vaikystėje tau teko žaisti su knygomis–žaidimais — tai tokios knygutės, kurių puslapiai suskaidyti į daug pastraipų, o jas skaityti reikia tam tikra

http://aol.com/ — amerikietiškoji AOL atstovybė.
http://corp.aol.com/ — korporacijos „America Online“ svetainė.
http://television.aol.com/ — internetinis televizijos kanalas IN2TV.
http://staff.jccc.net/lcline/index.htm — AOL diskų kolekcionieriai.
http://aim.com — populiarus AOL produktas, skirtas bendravimui internete (AOL Instant Messenger).
http://discover.aol.com/international.adp — tarptautinės paslaugos.


Žaidimų priedas Atari 2600


Džimas Kimsis — vienas pirmųjų AOL vadovų

tvarka. Tu dalyvauji visuose autoriaus aprašytuose veiksmuose — meti kauliuką ir savarankiškai pasirenki, kaip pasielgti tavo herojui. AOL tokius žaidimus perkėlė į kompiuterį ir greitai pristatė pirmąją seriją, kuri vadinosi QuantumLink Serial. Jos autoriumi tapo amerikiečių rašytojas Treisis Rydas. Po to atsirado ir Quantum Space — pirmasis visiškai automatizuotas žaidimas, žaidžiamas elektroniniu paštu. Ir, žinoma, pirmasis pasaulyje grafinis MMORPG — legendinis Neverwinter Nights, bendras „America Online" ir „Stormfront Studios" kūrinys. Šis online žaidimas, pagrįstas D&D rolių sistema, buvo pateiktas visuomenei 1991 metais ir egzistavo iki pat 1997 metų. Reikia pasakyti, kad jis buvo labai populiarus.

Augant kompanijai, AOL savo atstovybes kūrė ir kitose šalyse. Įdomią istoriją galima papasakoti apie AOL bandymą įžengti į Rusiją, kur kompanijos laukė liūdna baigtis. Pradėjus dirbti 1996 metais, rusiškoji AOL susidūrė su masiniais sukčiavimo su apskaita atvejais. Kovoti su tuo buvo nerealu, todėl kompanija nusprendė visiškai kapituliuoti, taip ilgam prarasdama viltis užkariauti didžiąją rytų rinką.

Susiliejimų periodas

Pirmojoje 90-ųjų pusėje „America Online" greitai augo ir plėtojosi. Rinkoje atsirado daug konkuruojančių kompanijų, tokių, kaip GEnie — General Electrics online paslauga, Prodigy — namų kompiuteriams skirta dialup paslauga, CompuServe. AOL ieškojo naujų sprendimų, kurių neturėjo kiti tiekėjai — kompanijos analitikai pasiūlė atsisakyti valandinio mokėjimo ir pakeisti jį fiksuotu mėnesiniu mokesčiu ($19,99). Tai ir tapo pirmąja stambia nesėkme. Kompanija tikėjosi trijų metų bėgyje po perėjimo prie naujo tarifo savo vartotojų skaičių padidinti 10-čia milijonų žmonių, tačiau iš tiesų viskas nutiko kiek kitaip. Į AOL vienu metu bandė prisijungti daugybė žmonių, linijos buvo mirtinai perkrautos, todėl tiekėjas pradėjo praradinėti klientus. Vartotojams greitai atsibodo girdėti trumpą užimtos linijos signalą, todėl jie nutraukinėjo savo sutartis su AOL. Vartotojų perbėgimą kitur stiprino dar

CHRONOLOGIJA

SUNKU BŪTŲ NEĮVERTINTI AOL INDĖLIO Į KOMPIUTERIŲ INDUSTRIJOS (YPATINGAI ONLINE PASLAUGŲ SFEROS) PLĖTOJIMĄSI. KOMPANIJA TAPO VIENA PIRMŲJŲ, KURI SUVOKĖ NAUJOS VERSLO SFEROS PERSPEKTYVUMĄ, IR NUO TO LAIKO JOJE UŽĖMĖ LYDERIO POZICIJAS. GERIAUSIAI APIE „AMERICA ONLINE" PLĖTOJIMOSI ETAPUS PAPASAKOS TRUMPA CHRONOLOGIJA.

1992/ **Kovas** — NASDAQ biržoje pradėtos pardavinėti pirmosios AOL akcijos (pavadinimas — AMER), vieneto kaina siekė $11,50.
1993/ **Gruodis** — „America Online" vartotojų skaičius viršijo 500 000 žmonių.
1994/ **Rugpjūtis** — AOL vartotojų skaičius viršijo milijoną.
1995/ **Vasaris** — AOL nupirko komercinį interneto tiekėją ANS. Klientų skaičius siekia 2 milijonus.
Gruodis — Klientų skaičius perlipo 4,5 milijono ribą.
1996/ **Sausis** — atidarytos kompanijos atstovybės Kanadoje ir Didžiojoje Britanijoje.
Rugpjūtis — daugiavartotojiškų žaidimų sferos plėtojimui nupirkta ImagiNation Network.
1997 / **Vasaris** — su „Tel-Save Holdings" sudarytas sandėris, kurio suma viršija 100 milijonų dolerių.
Lapkritis — AOL paslaugomis naudojasi daugiau nei 10 milijonų žmonių. Kompanija per vieną dieną apdoroja daugiau laiškų (elektroniniu pavidalu), nei JAV pašto tarnyba.
1998/ **Vasaris** — AOL pilnai prisijungia savo seną konkurentą — kompaniją „CompuServe".
Spalis — pradėjo veikti „AOL-Australia".
Gruodis — įvairias AOL paslaugas naudoja daugiau nei 15 milijonų vartotojų.
1999/ **Sausis** — pradėtas bendras su „Bell Atlantic" projektas dėl DSL ryšio paslaugų tiekimo.
Kovas — užbaigtas „Netscape Communications Corporation" prijungimas, nuo šiol Netscape naršyklė yra AOL nuosavybė.
Liepa — pradėtos teikti ADSL paslaugos.
Rugpjūtis — praėjus 14 mėnesių nuo to, kai AOL įsigijo ICQ, užsiregistravusių vartotojų skaičius padidėjo trigubai — iki 40 milijonų. Tą patį mėnesį išleidus AIM 3.0 — „naujos kartos" versiją — vartotojų skaičius pasiekė 45 milijonus.

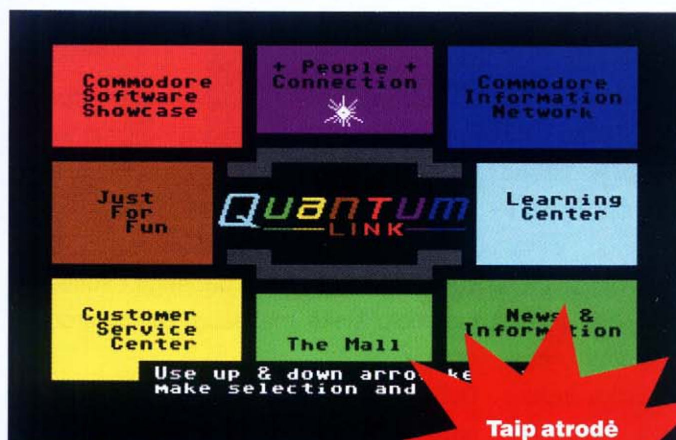
ir tai, kad „America Online“ neskubėjo savo klientams suteikti laisvo priėjimą prie WWW. Prieinami buvo tik tie tinklo servisai, kuriuos pripažino kompanijos klientinės programos. Pirmavimo palmės šakelė naujoviškumo atžvilgiu iš AOL rankų taip pat pereidavo pas kitas kompanijas. Išimtimi galima pavadinti idėją sukurti „Draugų sąrašą“ (Buddy Lists), kuri buvo postūmis pirmosioms internetinių pokalbių (IM — instant messaging) programoms.

Antroji rimta nesėkmė kompanijos laukė 2001 metais, kai AOL susiliejo su „Time Warner“ grupe. Šio visoje verslo istorijoje stambiausio susijungimo idėjos esmė buvo ta, kad taip būtų sutvirtintos pašlijusios AOL kaip tiekėjo pozicijos ir sukurtas milžiniškas interneto mediaholdingas, kuris turėjo šioje sferoje padaryti tikrą revoliuciją. Tačiau 90–ųjų interneto bumas atslūgo, susidomėjimas šiuolaikinių technologijų industrija taip pat sumažėjo, todėl tokie grandioziniai lūkesčiai paprasčiausiai nepasiteisino — abi kompanijos patyrė milžiniškų nuostolių. Buvo kalbama, kad „Time Warner“ iš viso ruošėsi nutraukti bendradarbiavimą, tačiau magnatas tik pakeitė savo pavadinimą. Po trijų metų egzistavimo su „AOL Time Warner Inc.“ pavadinimu jis vėl tapo „Time Warner Inc.“ Kompanijos atstovai tai pakomentavo taip: „AOL santrumpa neturėtų negatyviai veikti likusių korporacijos veiklos sferų ir bendro įvaizdžio“. Savo aktyvaus vystymosi laikotarpiu AOL įsiurbė nemažai kitų kompanijų: savo seną konkurentą „CompuServe“, „Mirabilis“ (ICQ kūrėjai), „Nullsoft“ („WinAMP“ kūrėjai), „Netscape“ ir daugelį kitų. Tačiau ne visi pirkiniai buvo sėkmingi. Po to, kai 1999 metais AOL už 4,2 milijardus dolerių įsigijo „Netscape“, tarp AOL ir „Microsoft“ prasidėjo rimtas teisinis aiškinimasis. AOL Geitsą ir jo kompanjonus apkaltino nesąžininga konkurencija, dėl kurios jų naršyklė Netscape tapo nepopuliaria. Tai reiškia, kad firmos Netscape pirkimui išleisti pinigai buvo išmesti vėjais. Procesas truko 16 mėnesių ir baigėsi taikos susitarimu, pagal kurį „Microsoft“ suteikė AOL teisę septynerius metus nemokamai naudotis naršykle Internet Explorer bei draugystės ir amžinos meilės vardan išmokėjo kuklią 750 milijonų dolerių sumą. Dalis šios sumos buvo skirta AOL skoloms padengti, kurios tuo metu siekė maždaug 20 milijardų dolerių.

Dabar „America Online“ reikalai klostosi neblogai. Susidaro įspūdis, kad ši korporacija nepaskandinama. Kad ir kas nutiktų, AOL vis tiek toliau veikia ir plėtojasi. Tarkim, 2005 metais buvo pastebėtas netikėtas susidomėjimo kompanijos paslaugomis augimas, o metų pabaigoje buvo sudarytas sėkmingas sandėris, po kurio AOL atiteko 5% „Google“ akcijų. Taip pat neseniai pasaulį išvydo AOL naršyklė, kuri iš esmės yra nemokamas IE skirtas apvalkalas. 2006 metų kovą pradėjo veikti naujas bendras AOL ir „Warner Bros Television“ projektas — IN2TV. Tai nemokama AOL abonentams skirta online televizija, transliuojanti populiarias televizijos laidas su komercinėmis pertraukėlėmis.

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

2000/ Atidarytos AOL atstovybės Meksikoje ir Argentinoje. AOL įsigyja „iAmaze“, „MapQuest Inc.“, „Quack.com“.
2001/ **Sausis** — kompanija pradeda teikti paslaugą Mail Alerts, leidžiančią tekstinį pranešimą išsiųsti į mobilųjį telefoną arba pranešimų gaviklį.
Gegužė — kartu su WebMD prasidėjo paslaugos, teikiančios įvairią informaciją apie sveikatos apsaugą ir įvairias šio tipo paslaugas milijonams online vartotojų, kūrimas.
Tą patį mėnesį AOL vartotojai pasiekia rekordą, internetinėse parduotuvėse pirkiniams išleisdami 6,7 milijardo dolerių.
Gruodis — išleidžiamas ICQ Lite, suteikiantis priėjimą prie savo ICQ su bet kokia naršykle, taip pat ir Mac OSX sistemoje veikianti ICQ versija.
2002 >> **Balandis** — su „Motorola“ sudaryta sutartis įtraukti AIM į kompanijos gaminamus telefonus.
Spalis — pradėta teikti paslauga AOL AMBER, skirta palengvinti internetinę dingusių arba pagrobtų vaikų paiešką.
2003/ **Balandis** — AOL per vieną dieną blokuoja 2 milijonus spamerių adresų.
2004/ **Vasaris** — pradėta teikti AOL paslauga jaunimui, kuri vadinasi RED.
Spalis — AOL savo klientams siūlo nemokamą antiviruso paketą.
2005/ **Balandis** — pradėta teikti internetinės telefonijos paslauga. AOL taip pat oficialiai praneša pradedanti karą prieš phishing'ą, dėl ko buvo pradėta atitinkama kampanija.
Rugpjūtis — nuperkama „XDrive Inc.“ — stambiausia duomenų saugojimo bei informacijos rezervinio kopijavimo paslaugų tiekėja, ir „Wildsteel Ltd.“ — pirmaujantis alternatyvių belaidžių sprendimų kūrėjas.
Rugsėjis — išleistas AOL tinklo apsaugos programų paketas, skirtas padidinti jos klientų saugumą.
Spalis — AOL prisijungia kompaniją „Weblogs“, interneto blogų rinkos lyderį.
Lapkritis — kompanija pristato AIM Triton — naujos kartos programą bendravimui.
Gruodis — AOL nuosavybe tampa viena pirmoji vaizdo klipų paieškos sistema Truveo.
2006/ **Balandis** — kompanija oficialiai pakeitė savo pavadinimą iš „America Online“ į AOL.



Taip atrodė Q-Link meniu



Spameriški AOL diskai

Nepaisant to, kad dialupas miršta ir tampa praeitimi, AOL, kaip Energizer, toliau dirba, dirba ir dirba, išbandydama save naujose online verslo sferose bei pradėdama naujus, tegu ir ne visada sėkmingus, projektus.

Liaudis prieš AOL

Su „America Online" vardu susiję daug skandalingų epizodų, kuomet situacija dažnai tapdavo visiškai absurdiška.

Nėra tokios programinės įrangos, kurios kas nors nebandytų nulaužti, tačiau AOL programos hakeriams buvo ypatingai gardus kąsnelis. Žymiausią „America Online" programų laužimui skirtą paketą 1994 metais sukūrė hakeris Da Chronic. Jo kūrinys vadinosi AOHell, jame buvo visi „būtiniausi" dalykai: nuo vartotojų vardų generatorių (paprastai jie veikdavo nuo 2 iki 4 savaičių) iki vartotojo vardo/slaptažodžio gavimui apgaulės būdu skirtų programų, kurios AOL vartotojams pranešimus išsiųsdavo darbo su klientais skyriaus vardu. Ten taip pat buvo spamo bombos, flood skriptai ir daugelis kitų dalykėlių.

AOL visada teikė pirmenybę agresyviai savo paslaugų ir programų reklamai. Pavyzdžiui, labiausiai pamėgtas savireklamos būdas buvo diskų su bandomosiomis versijomis siuntinėjimas paštu milijonams žmonių. Bandomosios versijos porai valandų suteikdavo nemokamą priėjimą prie vieno ar kito serviso. Kompanijos siuntinėjamas spamas taip visiems įgriso, jog susikūrė organizacijų, pasisakančių prieš tokią AOL politiką. Žymiausia jų vadinosi „No More AOL CDs!". Surinkę daugiau nei milijoną AOL diskų, šie vaikinai pamėgino visą šį gėrį išversti prieš kompanijos pagrindinę būstinę. Atseit, susirinkit savo šlamštą. Spaminę viešųjų ryšių strategiją kompanija nutraukė tik po keleto metų, o dabar tie diskai laikomi kolekciniais.

Dėl blogo prisiskambinimo, palaikymo sistemos ir kitų nesklandumų daugelis vartotojų buvo ryžtingai nusiteikę atsisakyti AOL ir pereiti pas kitus tiekėjus. Tuomet kompanija sukūrė ištisą personalui skirtą premijų ir priedų sistemą. Jiems skirta užduotis buvo paprasta: bet kokiais būdais atkalbėti vartotojus nuo paslaugų atsisakymo. Visa tai išplaukė į paviršių tuomet, kai Niujorko prokuratūra gavo daugiau nei 300 skundų dėl AOL darbo su klientais skyriaus. Tyrimas parodė, kad labai dažnai vartotojų abonentai toliau veikdavo net ir nepaisant vartotojų norų atsisakyti paslaugų — AOL darbuotojai paprasčiausiai ignoruodavo klientų prašymus.

2005 m. rugpjūčio 4 dieną „America Online" Niujorko valstijai išmokėjo 1,25 milijono dolerių baudą ir sutiko peržiūrėti savo darbo principą. Tuo tarpu už valstijos ribų gyvenantiems žmonėms tenka kankintis ir šiandien. Geru tai iliustruojančiu pavyzdžiu galėtų būti atvejis, nutikęs 2006 m. birželio 13 dieną. Žmogus, vardu Vincentas Ferari, internete pateikė telefoninio pokalbio su AOL operatoriumi įrašą, kur buvo kalbama apie abonemento atsisakymą. AOL operatorius, kuris prisistatė Džonu, atsisakė uždaryti Vincento abonementą, kol jis išsamiai nepapasakos, kuo jo netenkina tiekėjas ir ko jam trūksta. Peržiūrėjęs statistiką, operatorius pareiškė, kad jeigu visą pastarąjį mėnesį abonementu buvo naudotasi, reiškiasi nėra priežasčių nutraukti sutartį. Į visus AOL darbuotojo įkalbinėjimus trisdešimtmetis Vincentas atsakydavo kategoriškai „ne" — jis tiesiog norėjo atsisakyti savo abonento. Tuomet Džonas atsakė, kad jam reikalingas tėvų sutikimas ir kad jis šnekėsis tik su Vincento tėvu. Kai įrašas pakliuvo į telekanalo CNBC rankas, žurnalistai atliko eksperimentą: jie paskambino į AOL darbo su klientais tarnybą ir taip pat pabandė anuliuoti abonementą. Visa istorija pasikartojo, dėl ko abonemento atsisakymui prireikė 45 minučių aiškinimosi su operatoriumi. Istorija plačiai nuskambėjo internete ir spaudoje, dėl ko „America Online" buvo priversta atsiprašyti Vincento.




tango



100K/ tūkstančių tobulybės poligonų

PAŽINTIS SU PAČIOMIS PAČIAUSIOMIS VIRTUALIOMIS GRAŽUOLĖMIS

AR GALIMA ĮSIMYLĖTI VIRTUALŲ PERSONAŽĄ? ŽINAU, KAD TU DABAR PRADĖSI PURTYTI GALVĄ IR MANE ĮTIKINĖTI, KAD TU NE TOKS IR KAD MERGINOS, KURIAS BE VISO KITO GALIMA PAČIUPINĖTI IR NE TIK, TAVE JAUDINA LABIAU. ANKSČIAU AŠ IR PATS TAIP GALVOJAU, TAČIAU RUOŠIANT ŠĮ STRAIPSNĮ, KUOMET TEKO PERŽIŪRĖTI ŠIMTUS NUOTRAUKŲ IR DEŠIMTIS FILMUKŲ, MANO ŠIRDYJE PALENGVA UŽGIMĖ ABEJONĖ. MANAU, JOG TU JAU SUPRATAI, APIE KĄ BUS ŠIS STRAIPSNIS.

Kyoko Date

1996 metais japonų kompanija „Hori Pro Inc." pradėjo eksperimentinį projektą pavadinimu DK–96 (Digital Kids 96). Jo tikslas buvo išsiaiškinti, ar su 3D įrankiais sukurtas virtualus personažas gali išpopuliarėti tarp japonų jaunimo. Personažu, kurį per 2 metus sukūrė pirmaujanti japonų grafikos kompanija „Visual Science Laboratory", tapo šešiolikmetė dainininkė, vardu Kyoko Date. Vyresnioji suši baro savininkų dukra išaugo Fuzzos kvartale Tokijuje, vaikystėje žavėjosi futbolu ir žaidė mokyklos komandoje. Kyoko dievino mangą (japoniškus komiksus) ir pati neblogai piešė. Prieš pradėdama dainininkės karjerą panelė dirbo greito maisto restorane ir svajojo vieną kartą tapti žvaigžde. Vėliau ši virtuali istorija bus žinoma praktiškai visam japonų jaunimui.

1996 m. lapkričio 21 dieną buvo išleistas pirmasis muzikinis Kyoko Date singlas — „Love Communication". Kartu su



Rhona Mitra Laros Kroft pavidalu



Kyoko žurnalo viršelyje

juo buvo išleistas ir vaizdo klipas, kuriame Kyoko vaikšto po Tokijo ir Niujorko gatves. Daina greitai tapo populiari, ją suko pagrindinės radijo stotys, minios jaunimo plūdo į naujosios žvaigždės interneto svetainę ir reiškė susižavėjimą jos grožiu, grakštumu, balsu. „Ji nepriekaištinga, — sakė kūrėjai, — tarp realių žmonių nepriekaištingų nėra: kai kurie gerai dainuoja, bet atrodo nelabai, kai kurie gerai atrodo, bet blogai dainuoja. Kyoko turi visas scenos dievaičiui reikalingas savybes". „Hori Pro" pradėjo transliuoti naktinį radijo šou, kuriame dalyvavo Kyoko, ir jau ruošėsi organizuoti turą po Aziją. Tačiau Japonijoje gerbėjų širdyse scenos dievaičiai greitai gimsta ir taip pat greitai miršta. Taigi 1997 metų pradžioje japonų jaunimo susidomėjimas virtualia mergina pradėjo gesti.

Tuo metu apie japoniškąjį fenomeną sužinojo Amerika ir Europa. Ši tema pritraukė daugelio žymių leidinių žurnalistus, tačiau informacijos apie Kyoko anglų kalba praktiškai nebuvo — „Hori Pro" orientavosi išskirtinai į rytų rinką. Dėl to visas šis reikalas be trumpų interviu ir nedidelių pastabų toliau nepasistūmėjo.

Beje, būtent Kyoko Date įkvėpė Viljamą Gibsoną parašyti romaną „Idoru", kuriame viena pagrindinių herojų — virtuali superžvaigždė Rei Toei.

Aki Ross

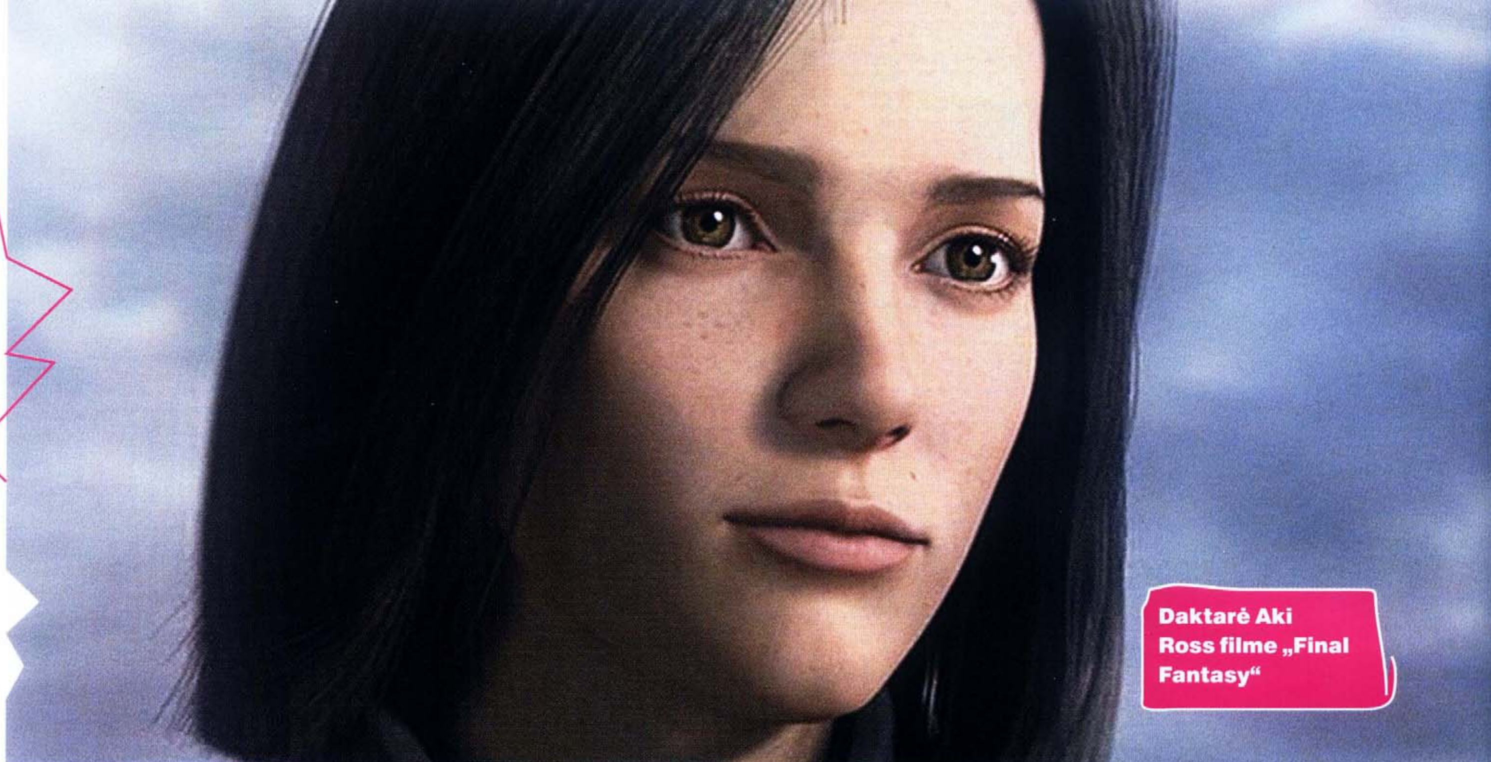
Daktarė Aki Ross — vienas pirmųjų kinematografo istorijoje fotorealistiškas personažas, kuris žinomas iš filmo „Final Fantasy: The Spirits Within". Šis kompanijos „Square Pictures", kuri dalyvavo kuriant grafiką Final Fantasy serijos žaidimams, šedevras buvo kuriamas ketverius metus įdarbinant 960 į vieną tinklą sujungtų Pentium III kompiuterių. Tuo metu, kai buvo kuriamos paskutinės scenos, teko perdarinėti pačias pirmąsias, kadangi jos jau spėjo pasenti ir išsiskyrė iš bendro vaizdo.

Filmo siužete žmonės kovoja su Fantomais — nežemiškomis gyvybės formomis, kurios iš kosmoso atkeliavo tam, kad sunaikintų bet kokią gyvybę. Aki Ross, kuri buvo užkrėsta Fantomais vieno susidūrimo metu, užsiima 8 dvasių paieškomis. Tik jie gali padėti sunaikinti ateivius ir išgydyti ją pačią, tačiau finale paaiškėja, kad raktas į žmonijos išgelbėjimą yra ne tik paslaptingos dvasios, bet ir pati Aki.

Kuriant filmą „Square Pictures" vardan iškelto tikslo — animacijos kokybę padaryti praktiškai neatskiriamą nuo realaus vaizdo — negailėjo nei priemonių, nei laiko. Keleto mėnesių prireikė vien tik 60 tūkstančių Aki plaukų modeliavimui. Prieš filmo išleidimą buvo manoma, kad fotorealistiški trimačiai personažai kinematografijoje padarys revoliuciją. „Square Pictures" planavo Aki Ross panaudoti kituose filmuose, įskaitant ir kombinuotus



Rytų gražuolė, nors ir netikra


Daktarė Aki Ross filme „Final Fantasy“

filmavimus su realiais aktoriais, tačiau už filmą gaunamos pajamos nepateisino kūrėjų vilčių, dėl ko jie atsisakė savo planų. 2001 metų spalį „Square“ net pareiškė apie savo išėjimą iš didžiojo kino pasaulio, tačiau šis išėjimas buvo neilgas. Vėliau buvo išleisti „Animatrix“, „Final Fantasy VII: Advent Children“ ir mažesni kompanijos projektai.

„Aki Ross“ ilgai pirmaujantiems 3D dizaineriams liko realistiškumo pavyzdžiu. Internetinėse diskusijose ji buvo laikoma moters grožio etalonu, o populiarus žurnalas „Maxim“ Aki net įtraukė į seksualiausių pasaulio gražuolių sąrašą, kur ji užėmė 87 vietą. Tai buvo pirmasis atvejis istorijoje, kada virtualus herojus rungėsi su realiomis moterimis.

Ananova

Mūsų pasaulis tapo tokiu progresyviu, kad šiandien vietoje realių žmonių televizorių ekranuose rodomi virtualūs. Pirmąja savo srityje virtualia vedančiąja tapo Ananova, kurią sukūrė naujienų agentūra „PA News“. Studijos dizaineriai nusprendė, kad tokia egzotika pritrauks papildomų lankytojų, ir jie pasirodė besą teisūs. Žmonės pradėjo šias naujienas žiūrėti ne tiek dėl pačių naujienų, kiek tam, kad paklausytų virtualios vedančiosios. Ananova tapo tokia populiari, kad „PA News“ savo naujienų resursą pervadino ananova.com.

Pasak agentūros, Ananovai 28 metai, jos ūgis — 170 centimetrų, jos plaukai žali, švelnus charakteris ir malonus balsas. Šiaip Ananova — tai iš karto dvi programos. Pirmoji atpažįsta ir įgarsina spausdintą tekstą, o antroji — valdo vedančiosios mimiką ir animaciją, taip sinchronizuodama ją su kalba. Svetainės lankytojas gali išsirinkti keletą transliavimo režimų: dviejų minučių skirtingų naujienų bloko skaitymą, naujienų pagal pasirinktus raktinius žodžius arba sportinės informacijos ir orų suvestinės skaitymą. Ši mergina tave taip pat gali perspėti elektroniniu paštu, jeigu tau įdomi tema nepakliuvo į naujienas arba kokia nors naujiena buvo atnaujinta. Svetainės administratoriai per virtualios vedančiosios darbo laiką gavo keletą tūkstančių Ananovai adresuotų lankytojų laiškų su pagyrimais, klausimais apie jos gyvenimą ir net pasiūlymais tekėti. Dabar ananova.com svetainės skyriuje „Video reports“ galima rasti skelbimą, kad paslauga „under construction“. Adminai tobulina merginos personažą, kad ji skambėtų ir atrodytų realistiškiau.

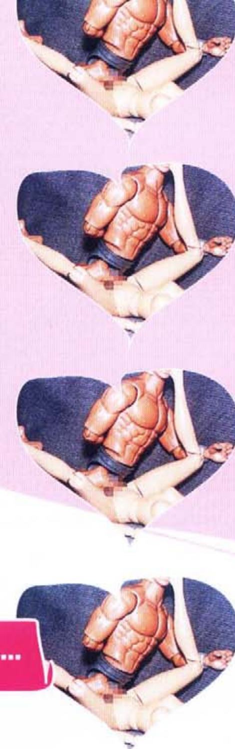
Webbie Tookay

Webbie Tookay visam pasauliui žinoma kaip pirmasis virtualus modelis. Jos ideali figūra gali pasigirti magiškais skaičiukais 90-60-90, o už tam tikrą sumą ji sutiks kokiai nors agentūrai parodyti madingus drabužėlius. Webbie gimimo metai — 1999, o jos tėvas yra firmoje „Illusion 2K“ dirbantis australų dizaineris Steven Stahlberg. Webbie nuo gimimo buvo lemta tapti modeliu. Bent jau tokią ateitį jai prognozavo jos kūrėjai. Iš karto po pristatymo viena prestižiškiausių pasaulio modelių agentūrų Elite su panele Tookay pasirašė sutartį. Jos nuotraukos pasirodė daugelyje žurnalų, ji vaikščiojo virtualiais



Pirmoji virtuali televizijos naujienų pranešėja Ananova





Kokios akys...

podiumais, o 2000 metais Webbie tapo brangiausiai apmokamu modeliu mados rinkoje. Jos metinės pajamos siekė 15 milijonų dolerių, o tai yra 10 milijonų daugiau už brangiausiai apmokamo gyvo modelio Gisele Bundchen gaunamas pajamas. „Mes tikimės, kad Webbie taps virtualių pramogų industrijos simboliu, o jos kaina bus skaičiuojama šimtais milijonų dolerių", — pasidalino savo mintimis su spauda „Illusion 2K" prezidentas. Patvirtindamas savo žodžius, jis paminėjo eilinę sutartį su „Nokia" korporacija, kuriai Webbie tapo interneto ir mobiliojo ryšio apjungimo simboliu.

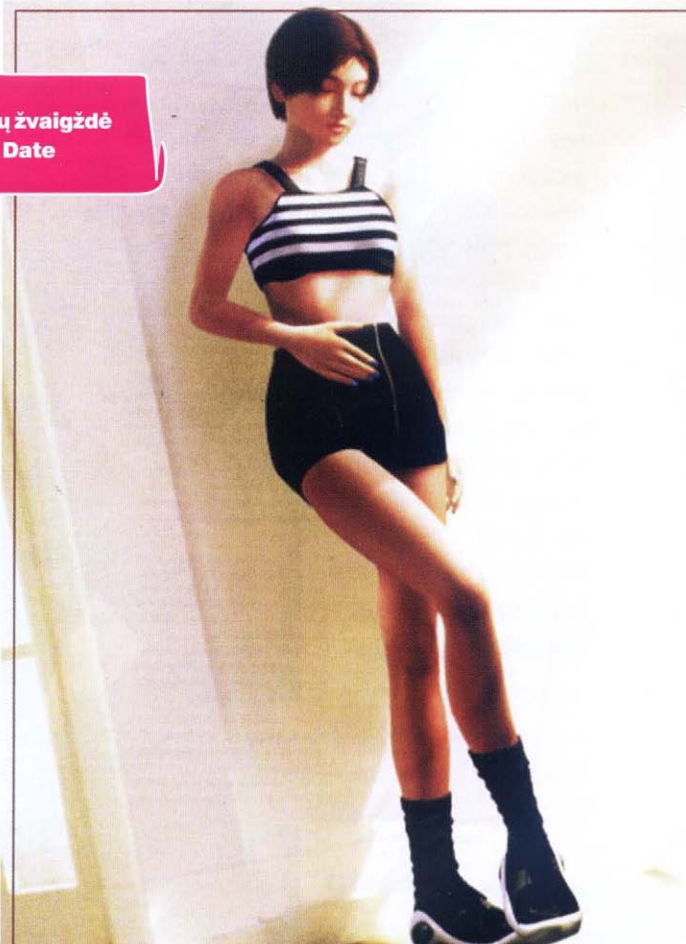
Nors Webbie neturi tikriems modeliams būdingų žalingų įpročių (rūkymas, alkoholis, rizika sustorėti arba susirgti), kaprizus jai paliko. Ji yra arši kovotojų už gyvūnų teises šalininke, todėl jokiu būdu neužsidės drabužių su kailiais. Mergina taip pat dalyvavo RSA rakto nulaužimo projektuose.

Kai Webbie tapo pakankamai žinoma, „Illusion 2K" pradėjo keletą naujų projektų: „Webbie Planet" — kompiuterinis šou su Webbie, kuriame ji kreipiasi į realias ir virtualias įžymybes, „Webbietainment" — belaidė interneto paslauga, į mobiliuosius telefonus transliuojanti naujienas su visiems pažįstama vedančiąja, „Webbie Mascot" — interaktyvus agentas, padedantis vartotojams ieškoti informacijos, gauti paštą ir t.t., XX0 — muzikinė grupė iš virtualių modelių, kuriems vadovauja Webbie, „What We Wear" — virtuali parduotuvė, kurioje taip pat neapsieita be trimatės merginos.

Dabar Webbie jau toli gražu ne vienintelis virtualus modelis. Pavyzdžiui, Prancūzijoje „Ford" modelių agentūra įdarbino trimatę Eve Solal. Mergina taip išpopuliarėjo, kad ketvirtadieniais per radiją veda nuosavą šou. Bėgant metams Webbie šlovė šiek tiek nurimo — dabar ji žinoma ne kaip pats vertingiausias modelis, o kaip pirmasis virtualus personažas, patyręs komercinę sėkmę realiame versle.

Kaya

Ko gero, niekam kuriant virtualią merginą dar nėra pavykę pasiekti tokio realistiškumo lygio, kaip Kaya autoriui. Brazilijos 3D modeliuotojo Alceu Baptistao herojė nepretenduoja į pačios karščiausios pupytės titulą — jos nosytė riesta, veidą puošia strazdanos, didelė burna. Nepaisant to, ji miela ir patraukli, tačiau svarbiausia tai, kad nepaprastai tikroviška. Ant jos veido odos net galima matyti poras. Projektas kol kas dar tik plėtojamas: Kaya dar neturi kūno, o pats autorius, norėdamas sutaupyti laiko plaukų modeliavimui, merginos galvą uždengė paprasčiausia berete. Tačiau



Japonų žvaigždė Kyoko Date



jau dabar galima įvertinti Alceu darbą pagal nuotraukas ir trumpą filmuką, kur Kaya pasakoja apie save.

Praktiškai visi modelio elementai buvo sukurti su 3D paketu Maya panaudojant standartinius filtrus. Beje, tekstūros buvo piešiamos ranka, o ne paimamos iš padarytų nuotraukų. Kaip sako Alceu, Kaya kuriama animaciniams tikslams, todėl visi pagrindiniai elementai kuriami trimačiame pakete.

Projektas nėra komercinis — Baptistao prie jo dirba laisvu nuo pagrindinio darbo laiku (šiaip jis yra FX kompanijos „Vetor Zero" direktorius). Autorius planuoja savo merginą padaryti interaktyvia, taigi bet kuris svetainės lankytojas galės valdyti jos emocijas ir judesius bei su ja pabendrauti. Tolimesnėje ateityje planuojama jai surasti darbą šou, kino versle arba kur nors kitur.

O apie Kaya „grožio netobulumą" vienas žymus 3D modeliuotojas yra pasakęs: „Daugelis dizainerių vaikosi idealaus grožio, tačiau jie nesupranta, kad tai jų personažų nepadaro iš tikrųjų gyvais. Nedidelių trūkumų galima rasti bet kurio žmogaus išorėje, todėl tikrasis meistriškumas — savo herojei suteikti tokių bruožų, kurie priverstų žmones patikėti jos realistiškumu, tuo pačiu suteikiant jai charizmos".

Beje, Kaya pelnė keletą apdovanojimų, įskaitant ir Vokietijoje vykusio festivalio „Animago" Geriausio personažo titulą bei prizinę vietą Londono parodoje „Ateities veidai".





Webbie Tookay

Mika

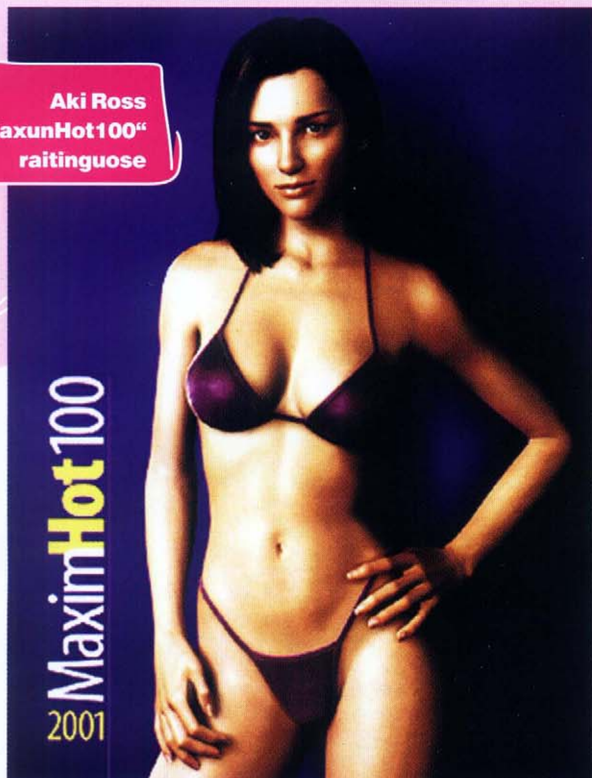
Mergina, kuri pavergė Londono paskutinių kibermoterų kūrimo pasiekimų parodą. Lankytojų nuomonės išsiskyrė, kas realistiškesnė — Kaya ar Mika. Mika Amore autoriumi tapo legendinis 3D dizaineris Rene Morelis, dirbęs prie filmo „Final Fantasy" ir šiek tiek prisidėjęs prie Aki Ross kūrimo.

Mika gyvena amazonsoul.com svetainėje — tai ambicingas projektas „suaugusiesiems", interaktyvių komiksų rinkinys, kurių herojai — seksualios trimatės merginos. Siužetas plėtojamas ateityje, Amazon visatoje, kurioje gyvena išimtinai moteriškos lyties atstovės. Čia tiesiog knibždėte knibžda karštų gražuolių, kurios važinėja su raketas primenančiais aparatais ir yra pamišusios dėl sekso. Agentė Mika supranta, kad šiame pasaulyje kažkas ne taip, todėl pradeda mitinės būtybės — „vyro" — paieškas, tačiau kelyje susiduria tik su kitomis sekso maniakėmis.

Savaime suprantama, norint nevaržomai mėgautis virtualios merginos nuotykiais,



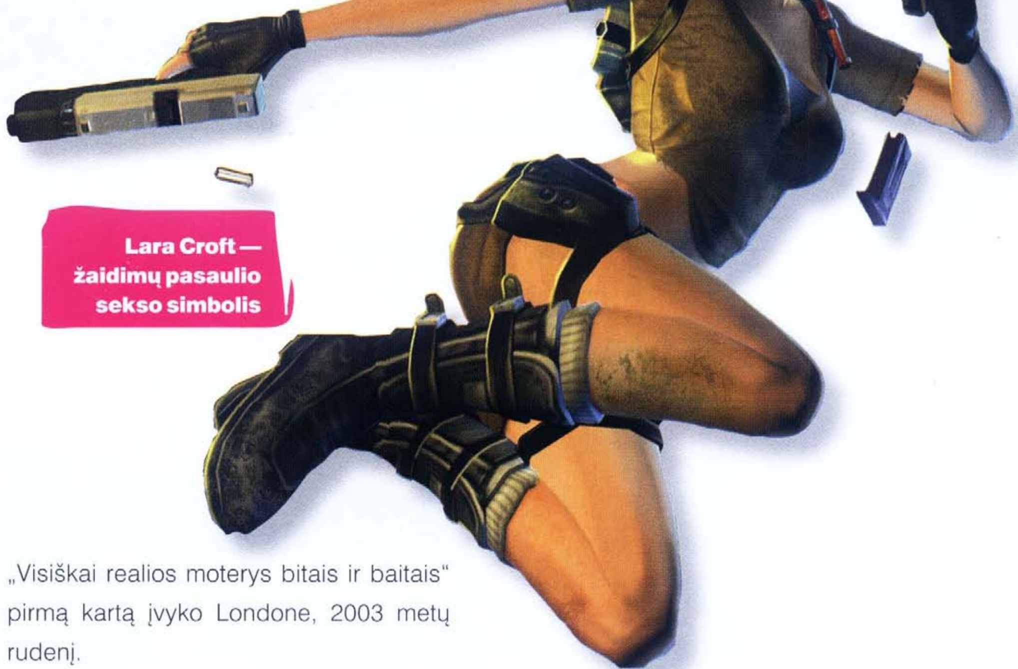
Seksualioji amazone Mika



Aki Ross „NaxunHot100" raitinguose



Dik — tas pats vaikinas, kuris pradingo amazonių gentyje



Lara Croft — žaidimų pasaulio sekso simbolis

teks pakloti šiek tiek pinigėlių ($10 per mėnesį). Nariai gauna pilną priėjimą prie visų puslapių ir interaktyvių galimybių. Pavyzdžiui, jie gali didinti/mažinti vaizdą, tam tikrose komikso dalyse įjungti animaciją ir net paveikti herojų gyvenimo eigą. Be Mikos Amazon Soul visatoje galima sutikti Karmą Shootrą — vyriausią juodu lateksu apsirėdžiusią slaptos sektos žynę, S — seksualią Karmos vergę, Neli — Amazon visatos paslapčių saugotoją, Dick'ą — kosminio laivo pilotą, kuris amazonių pasaulyje patiria avariją.

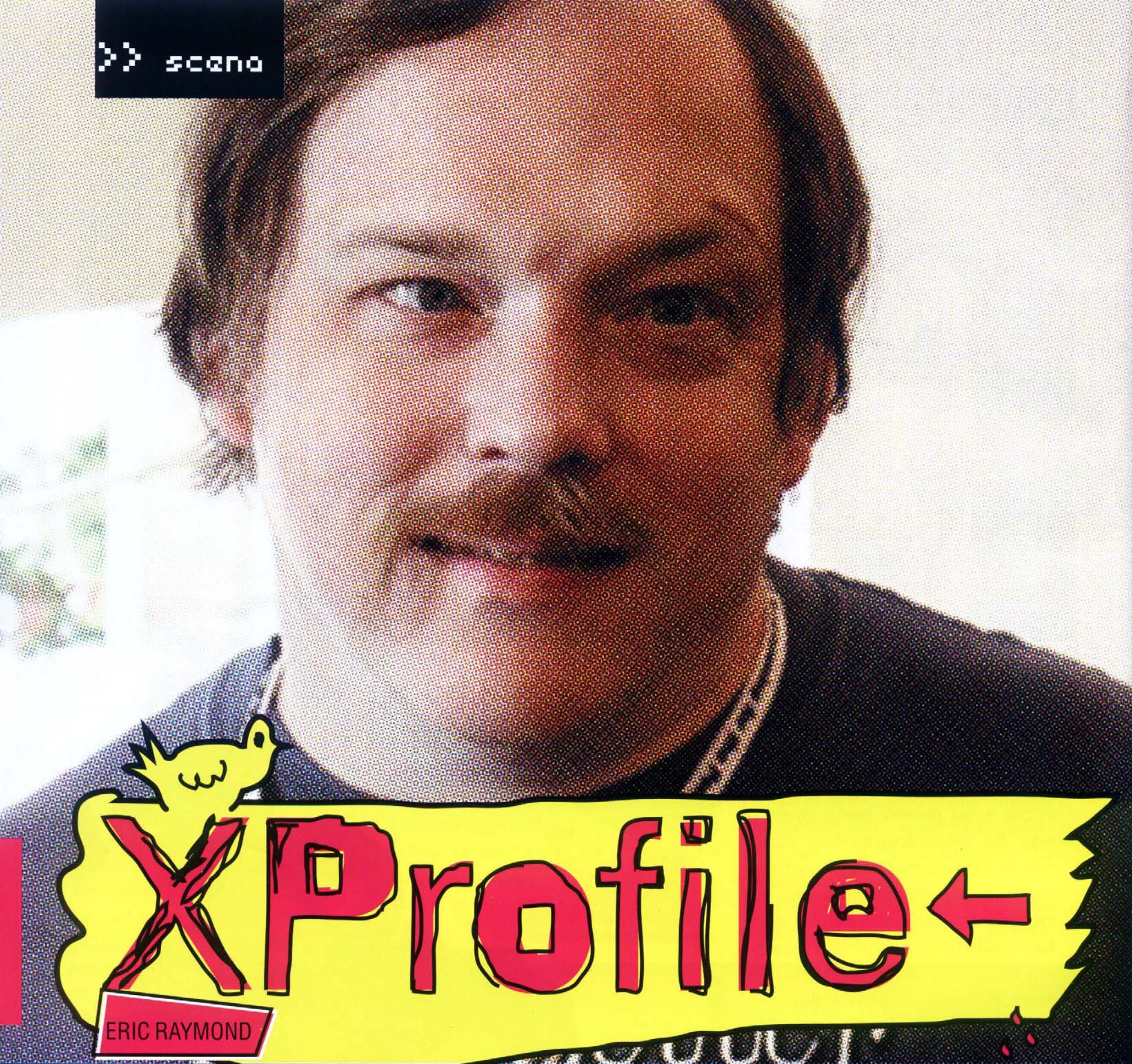
Šis projektas dar tik prasidėjo. Dabar kūrėjai yra paruošę apie 40 interaktyvių puslapių. Pasak svetainės savininkų, artimiausiu metu atsiras naujos dalys.

Kaip matai, susidomėjimas nuo gyvų žmonių neatskiriamų virtualių personažų kūrimu auga, o geriausiems 3D modeliuotojams tai tikras iššūkis. Jeigu anksčiau tokie dalykai dėl technologijų apribojimų buvo paprasčiausiai neįmanomi, tai dabar sukurti realistišką trimatę gražuolę visiškai realu.

Pasaulyje kasmet vyksta įvairios parodos, kur pirmaujantys dizaineriai demonstruoja savo darbus. Pavyzdžiui, paroda „Visiškai realios moterys bitais ir baitais" pirmą kartą įvyko Londone, 2003 metų rudenį.

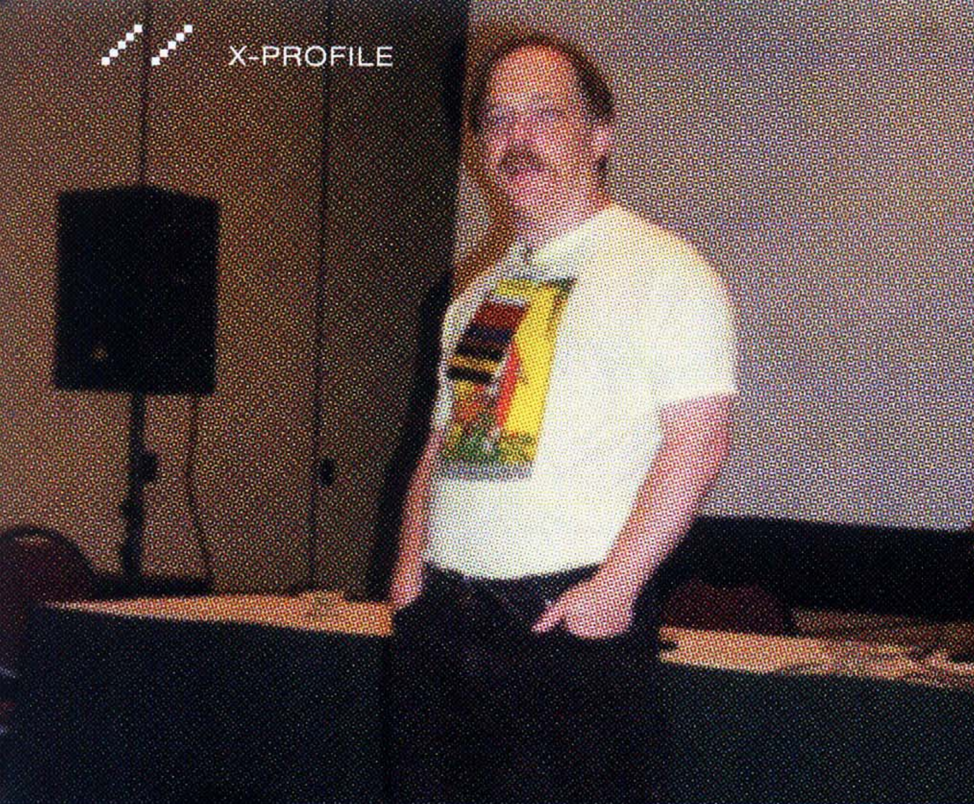
Taip pat jau vyksta virtualių gražuolių grožio konkursai. Sutikti tau jau pažįstamą Kaya, futuristinę Mika ir daugelį kitų personažų galima adresu www.missdigitalworld.com. Komisijos išrinktos karalienės autorius gauna 5 tūkstančius dolerių ir sutartį su „Cerami" agentūrą dėl modelio panaudojimo versle.

Ką gali žinoti, galbūt po keleto metų mes jau negalėsim atskirti, kur tikros merginos nuotrauka, o kur trimatis vaizdas. Galbūt netrukus realius aktorius ir dainininkus pakeis jų virtualūs prototipai. Pasaulis kinta pernelyg greitai, kad garantuotai žinotume, kas mūsų rytoj laukia.



Erikas gimė 1957 metais Bostone, šeimoje buvo vyriausias iš penkių vaikų. Jo tėvas dirbo sisteminiu Sperry UNIVAC programuotoju, todėl jam dažnai tekdavo persikelti iš vienos vietos į kitą. Dėl šios priežasties kai Reimondui sukako 14 metų, jo šeima spėjo pabuvoti trijuose kontinentuose, kol galutinai apsistojo Pensilvanijoje. Dėl to, kad Erikas sirgo lengva cerebralinio paralyžiaus forma, jis tapo savo klasiokų pajuokų objektu. Tiek dėl pastarosios aplinkybės, tiek ir dėl to, kad jis buvo auklėjamas pagal griežtas katalikiškas taisykles, jis jautė priešiškumą bet kokioms valdžios apraiškoms. Bėgant metams šis nenoras paklusti tik augo. Nepaisant ligos, Erikas buvo labai gabus vaikas, buvo gabus matematikai, fizikai ir muzikai. Pensilvanijos universitete dėstytojai manė, kad jis turi didelį potencialą, tačiau dėl disciplinos trūkumo ir nenoro laikytis oficialių reikalavimų Erikas aukštąją mokyklą baigė be jokio mokslinio laipsnio. Nepaisant to, universitete praleistas laikas nenuėjo veltui — Reimondas savarankiškai perprato programavimą ir kelerius metus dirbo keliose kompiuterių kompanijose. 1985 metais Erikas nusprendė, kad jis negali dirbti korporacijai, todėl išėjo iš darbo ir atsidavė žurnalistikai.

70-aisiais metais Erikas Reimondas susipažino ir susidraugavo su Ričardu Stolmanu, kuris jame uždegė meilę atviram kodui (open source). Erikas tapo vienu pirmųjų judėjimo už laisvą PĮ aktyvistų ir įnešė didelį indėlį į GNU projekto plėtojimą. Tarp pir-



90–ųjų pradžioje jis aktyviai dalyvavo GNU Emacs 19 projekte, užsiiminėjo lisp bibliotekų kūrimu, o nuo 1997 iki 1998 ėmėsi Sunsite (stambiausios pasaulyje Linux online programų saugyklos). Jis parašė programinę aplinką keeper, kuri svetainėje naudojama ir šiandien.

1998 metų vasarį Briusas Perensas ir Erikas Reimondas įkūrė organizaciją Open Source Initiative, kurios pagrindiniu tikslu tapo laisvos programinės įrangos populiarinimas. Reimondas buvo jos prezidentu iki pat 2005 metų ir taip atstovavo atviro kodo judėjimą spaudoje ir versle. Dėl savo aktyvumo jis per keletą metų tapo vienu iš esminių atviro kodo pasaulio figūrų. Tiesa, jo idėjos ne visada sutapdavo su kitų laisvos PĮ tėvų idėjomis. Erikas nesiliauja savo straipsniuose kritikavęs savo seno draugo Ričardo Stolmano, kur sako, jog jis per daug užsiiminėja retorika ir per mažai programuoja.

Reimondas taip pat dalyvavo keliuose mažiau žinomuose projektuose: BBS su priėjimu prie interneto Chester County InterLink, online programinės įrangos archyvas Trove, pcomm–2.0 — ProComm UNIX klonas, System V ir kituose.

Erikas Reimondas aktyviai pasisako už tai, kad žmonės pasauliniame tinkle laisvai reikštų savo mintis, siekdami saugumo naudotų ypač apsaugotus šifravimo metodus ir pasisakytų prieš politinę cenzūrą bei kontrolę. 2002 metų pavasarį jis pradėjo rašyti savo nuosavą web blogą (http://esr.ibiblio.org/?p=129) ir nuo to laiko šis puslapis tapo neišsenkančiu laisvų idėjų bei autorinių minčių šaltiniu apie Linux, technologijas, rasizmą ir karus.

Mane galima pavadinti hakerių pasaulio antropologu. Hakerių istorijos ir visuomenės studijavimas — svarbi mano gyvenimo dalis, beje, aš studijuoju ne techninę, o socialinę pusę.

Aš gyvenu tokios programinės įrangos pasaulyje, kurio niekaip negalėtum apibūdinti žodžiu „Sucks“. Taip yra todėl, kad aš viskam, ką bedaryčiau, naudoju Linux.

Projektai

Prieš savo viešą atsiradimą atviro kodo pasaulyje Erikas buvo žinomas kaip „Naujojo hakerių žodyno“ autorius. Iš esmės tai senas geras hacker's jargon file, kurį Reimondas iš kaip reikiant paredagavo ir papildė. Daugelis mano, kad Erikas šią bylą sugadino, kadangi įtraukė nuosavus techninius terminus ir atskiedė istoriją savo atviro kodo idealais. Kad ir kaip ten bebūtų, jis šio dokumento papildymais užsiiminėjo nuo 90–ųjų pradžios, o 1996 metais MIT Press leidykloje buvo išleista spausdintinė versija. Elektroniniu pavidalu ją galima rasti čia: http://catb.org/~esr/jargon. Be to, Erikas tapo dar dviejų žinomų knygų autoriumi: „Bažnyčia ir turgus“ (savotiškas atviro kodo ideologijos manifestas) ir „UNIX programavimo menas“. Kai 1998 metais kompanija „Netscape“ savo naršyklės kodą padarė laisvai prieinamą, jos atstovai prisipažino, kad šiam sprendimui juos įkvėpė Reimondo esė „Bažnyčia ir turgus“. Be jokios abejonės, tai paglostė Eriko savimeilę.

mųjų jo atviro kodo programų buvo pašto klientas Fetchmail, redaktorius Gosmacs, XFree86 vaizdo nustatymų konfigūratorius, VMS skirtas Solitaire, hex dumper, paprastas keyloggeris, programavimo kalbos INTERCAL ir CUPL, demonas gpcd ir t.t.

Hobiai

Lauko RPG (dalyvavo daugiau nei 30–yje stambių lauko RPG), kompiuteriniai Wargames, įvairios kovos menų rūšys: turi Moo Do (Taekwondo šaka) juodąjį diržą, praktikuoja aikido, kung fu ir sicilietiškas kovas su kalavijais. Erikas groja fleita, gitara, mušamaisiais ir net yra išleidęs porą albumų. Jis gerai išmano apie šaunamuosius ginklus ir nuolat praktikuojasi šaudyme. Erikas taip pat yra didelis mokslinės fantastikos gerbėjas. 90–ųjų pradžioje jis išleido keletą dešimčių mokslinės fantastikos knygų apžvalgų.

faq you faqing faq

HACK FAQ

Q: AŠ PAMIRŠAU ... SLAPTAŽODĮ. KĄ MAN DARYTI?

A: Tai labai populiarus klausimas. Būtent todėl šiame atsakyme aš specialiai surinkau nuorodas į visų pagrindinių įrankių, naudojamų laužti pamirštus populiariausių programų slaptažodžius, svetainių adresus. Toliau aš išvardinsiu tik nemokamas programas (*freeware*).

Dialupass (*www.nirsoft.net*) *Windows 2000/XP/2003* sistemose suranda standartiniuose *Dialup/RAS/VPN* įrankiuose įvestus slaptažodžius.

Mail PassView (*www.nirsoft.net*) atstato *Outlook Express*, *Microsoft Outlook 2000/2002/2003*, *IncrediMail*, *Eudora*, *Netscape Mail*, *Mozilla Thunderbird*, *Group Mail Free* pašto slaptažodžius.

The Bat! UnPass (http://tbup.boom.ru) atstato visų versijų *The Bat!* pašto dėžučių slaptažodžius.

Asterisk Logger (*www.nirsoft.net*) atstato po žvaigždutėmis (****) paslėptus slaptažodžius. Tokie slaptažodžiai naudojami daugybėje programų, pavyzdžiui, *CuteFTP*, *CoffeeCup Free FTP*, VNC, *IncrediMail*, taip pat *Outlook Express* ir *The Bat!*

LCP (*www.lcpsoft.com*) skirta *Windows NT/2000/XP/2003* sistemų vartotojų slaptažodžiams atstatyti.

MessenPass (*www.nirsoft.net*) atstato *ICQ Lite*, *Miranda*, *Trillian*, *MSN Messenger*, *Windows Messenger*, *Google Talk*, *AOL Instant Messenger* ir t.t. slaptažodžius.

Messenger Key (*www.lostpassword.com/messenger.htm*) skirta visų versijų ICQ slaptažodžiams atstatyti, pradedant ICQ 99 versija.

Protected Storage PassView (*www.nirsoft.net*) parodo slaptažodžius, kuriuos sistemoje išsaugo *Internet Explorer*, *MSN Explorer* ir *Outlook Express*. Šie slaptažodžiai nuskaitomi tiesiai iš *Windows Protected Storage*. Tai labai naudinga programa, kadangi ji gali padėti atstatyti pamirštus forumų, pokalbių svetainių, *web* parduotuvių, pašto dėžučių ir kitų *web* servisų slaptažodžius. Deja, man nepavyko surasti nemokamų programų, kurios laužtų apsaugotų archyvų ir *Microsoft Office* paketo programų slaptažodžius. Dėl to galiu tau pasiūlyti tik *www.passwords.ru* svetainę, kurioje tu rasi laikinai nemokamas ir demonstracines slaptažodžiais apsaugotų praktiškai visų archyvų (*RAR/WinRAR*, *ZIP/WinZIP*, *ARJ/WinARJ*, *ACE/WinACE*) ir *Microsoft Office 95/97/2000/XP/2003* dokumentų (ir daugelio kitų apsaugotų programų) slaptažodžių perrinkimo programų versijas.

Q: KUO IP SPOOFINGAS SKIRIASI NUO TCP SPOOFINGO?

A: Žodis „spoofing“ iš anglų kalbos verčiamas kaip apgaulė, apgavystė. Kaip tu tikriausiai pats supranti, apgaudinėti galima įvairiai. IP spoofingas, kaip reiktų suprasti pagal pavadinimą, susijęs su IP protokolu, TCP spoofingas — su TCP protokolu. IP spoofingas — tai siuntėjo IP adreso pakeitimas siunčiamuose paketuose. Hakeriai šį metodą dažnai naudoja tam, kad nuslėptų savo tikrojo buvimo (kitaip tariant, to mazgo, iš kurio atakuojama) vietą.

TCP spoofingas skirtas perimti susijungimą tarp aukos ir kito mazgo padirbant TCP paketus. Tokiu atveju aukos susijungimas pakimba, o atakuojantysis gali ramiai dirbti su šiuo mazgu, apsimesdamas auka. Norint realizuoti TCP spoofingą, hakeris turi sužinoti tarp aukos ir mazgo siuntinėjamų TCP paketų antraštėse naudojamų *Sequence Number* ir *Acknowledgment Number* laukų 32 bitų reikšmes (ISS — *Initial Sequence Number*). Jeigu hakeris ir auka yra viename potinklyje, tai šias reikšmes galima gauti pasinaudojus sniferiu. Senais gerais Mitniko laikais pradinę ISS reikšmę buvo galima atspėti, kadangi operacinės sistemos ją generavo pagal žinomus algoritmus. Norint perimti susijungimą reikėjo pasiųsti daugybę TCP užklausų su labiausiai tikėtinomis ISS reikšmėmis. Deja, mūsų laikais operacinės sistemos ISS generuoja atsitiktinai, todėl jų atspėti nepavyks. Rekomenduoju perskaityti vieną gerą apie tai rašantį straipsnį: *www.securitylab.ru/analytics/216199.php*.

Q: KAIP ĮSILAUŽTI Į SISTEMĄ, KURIOS LOGAI KOPIJUOJAMI Į NUTOLUSIĄ MAŠINĄ, IR TUO PAČIU NEIŠSIDUOTI?

A: Jeigu yra galimybė, laužimo metu su DoS'u atakuok tą kompiuterį, kuriame saugomi logai. Jeigu tu jį išvesi iš rikiuotės, jis negalės iš mašinos–aukos priiminėti logų. Jeigu logai kopijuojami su *syslogd*, tada tu gali panaudoti kitą būdą — užteršti logus suklastotais įrašais, čia tau padės programa *SYSLOG Fogger* (*http://packetstormsecurity.org*). Galų gale, pamėgink nulaužti patį logų serverį. Adminai gali nelabai atidžiai sekti tokio kompiuterio programinės įrangos atnaujinimus, todėl įma-

noma, kad loginančioje mašinoje pavyks rasti kokį nors seną produktą, kuriam skirti eksploitai voliojasi visame internete.

Q: GIRDĖJAU, KAD YRA TOKS DAIKTAS, VARDU „OBFUSKATORIUS". KAS ČIA TOKS?

A: Angliškas žodis „obfuscate" pažodžiui verčiamas kaip „supainioti", „suklaidinti", „užtemdyti". Obfuskacija — tai programos kodo supainiojimas, t.y. toks išeities teksto arba vykdomo kodo transformavimas, kuris išsaugo programos funkcionalumą, tačiau apsunkina jų analizę ir modifikavimą. Obfuskuoti galima rankiniu būdu arba šią užduotį pavesti specialioms programoms — obfuskatoriams. Obfuskacija dažniausiai naudojama tokiose programose, kurios platinamos su išeities tekstais ir yra parašytos su tokiomis kalbomis, kaip *JavaScript*, *VBScript*, *Perl* ir net HTML. *Java* ir .NET platformos kalbos išeities tekstą kompiliuoja į tarpinį kodą (baitkodą), kuriame yra pakankamai informacijos, kad būtų galima atstatyti pradinį išeities tekstą. Dėl pastarosios priežasties šiose kalbose taip pat dažnai naudojama tarpinio kodo obfuskacija. Paprasčiausias obfuskuoto HTML pavyzdys: *<i>hak</i><i>eris</i>*. Naršyklėje bus parodytas žodis „hakeris", o išeities tekste tokio žodžio nėra.

Be programų apsaugos nuo analizės ir modifikavimo, obfuskatoriai paprastai optimizuoja programos dydį ir darbo greitį. Java skirtų obfuskatorių pavyzdžiai: *ProGuard* (*http://proguard.sourceforge.net*) ir *JavaGuard* (*http://sourceforge.net/projects/javaguard*).

Q: SU C RAŠAU BRUTFORSERĮ IR NORIU Į JĮ PRIDĖTI GALIMYBĘ PERRINKINĖTI SLAPTAŽODŽIUS PER SSL BEI SSH, TAČIAU NEMAČIAU JOKIOS LITERATŪROS, KURI PAAIŠKINTŲ, KAIP TAI DARYTI. KĄ SIŪLYTUM?

A: Į programą pridėti SSL ir SSH galimybę visiškai nesudėtinga. Paprastai tam naudojamos atskiros bibliotekos, pavyzdžiui, *OpenSSL* (*www.openssl.org*) arba *libssh* (*http://0xbadc0de.be/libssh/libssh-0.11.tgz*).

Archyvuose su bibliotekomis būtinai pateikiamos ir programuotojams skirtos instrukcijos (anglų kalba), kuriose aiškinama, kaip šias bibliotekas prijungti ir naudoti programose. Keleto bibliotekinių funkcijų iškvietimų pakanka, kad tavo programa panaudotų visą šių protokolų galią.

Q: KAS TAI YRA MALWARE?

A: Terminas „malware" yra *Malicious Software* trumpinys, kas verčiama kaip „piktavališka/kenkėjiška programinė įranga". *Malware* sąvoka aprėpia virusus, kirminus, trojanus, rootkitus, keyloggerius ir kitą hakerišką bjaurastį, kuri sutrikdo normalų kompiuterio darbą.

Q: KAIP WINDOWS XP SISTEMOJE PERŽIŪRĖTI ATIDARYTAS JUNGTIS, BYLAS, KAS IR KOKIUS PROCESUS PALEIDĘS IR T.T. ŽODŽIU, KAIP ATLIKTI PILNĄ SISTEMOS AUDITĄ IR TAIP PATIKRINTI, AR JOJE NĖRA TROJANŲ BEI KITOKIŲ NEKVIESTŲ SVEČIŲ?

A: Aš tau papasakosiu tik apie standartines XP komandinės eilutės priemones. Su įrankiu *netstat* galima gauti informaciją apie atidarytas jungtis ir užmegztus susijungimus. Raktas *–a* parodo visas aktyvias ir klausomas jungtis. Raktas *–o* parodo TCP arba UDP jungtis atidariusių procesų identifikatorius (PID). Raktas *–n* adresus ir jungčių numerius atvaizduoja skaitmeniniu formatu, t.y. nebando atlikti vardų transliavimo. Įrankis *tasklist* parodo sistemoje paleistus procesus ir jų identifikatorius (PID). Raktas */m* parodo kiekvieno proceso užkrautas DLL bibliotekas. Raktas */svc* parodo kiekvieno proceso paleistus servisus. Raktas */v* pateikia išsamesnę informaciją (*verbose*). Įrankis *taskkill* leidžia naikinti (*kill*) procesus. Įrankis *qwinsta* pateikia XP sistemoje užsiregistravusių (prisiloginusių) vartotojų sąrašą. Įrankis *qprocess* parodo kiekvieno užsiregistravusio vartotojo paleistų procesų sąrašą. Įrankis *openfiles* parodo per tinklą atidarytas bylas. Raktas */disconnect* leidžia uždaryti tiek nutolusio, tiek ir lokalaus vartotojo atidarytas bylas. Įrankis *systeminfo* pateikia sistemos konfigūracijos duomenis. Raktas */s* leidžia šią informaciją gauti iš nutolusių mašinų.

Q: AR MŪSŲ LAIKAIS HAKERIUI REIKIA MOKINTIS PERL?

A: Jeigu kalbi apie tikrą hakerį, tuomet jis turi mokintis bei studijuoti viską, kas susiję su kompiuteriais ir tinklinėmis technologijomis, juo labiau tokią žinomą kalbą, kaip *Perl*. Visai kitas klausimas, kokia tvarka visa tai daryti. Iš pradžių nuspręsk, kam tau reikalingas *Perl*? Jeigu tu ruošiesi užsiimti svetainių laužimu ir defeisais, tuomet, savaime suprantama, pirmiausia pradėk nuo *Perl*. Tiesa, mūsų laikais *Perl* populiarumą smarkiai sumažino tokios *web* kalbos, kaip PHP ir ASP, tačiau vis tiek pasauliniame voratinklyje ji vis dar aktyviai naudojama.

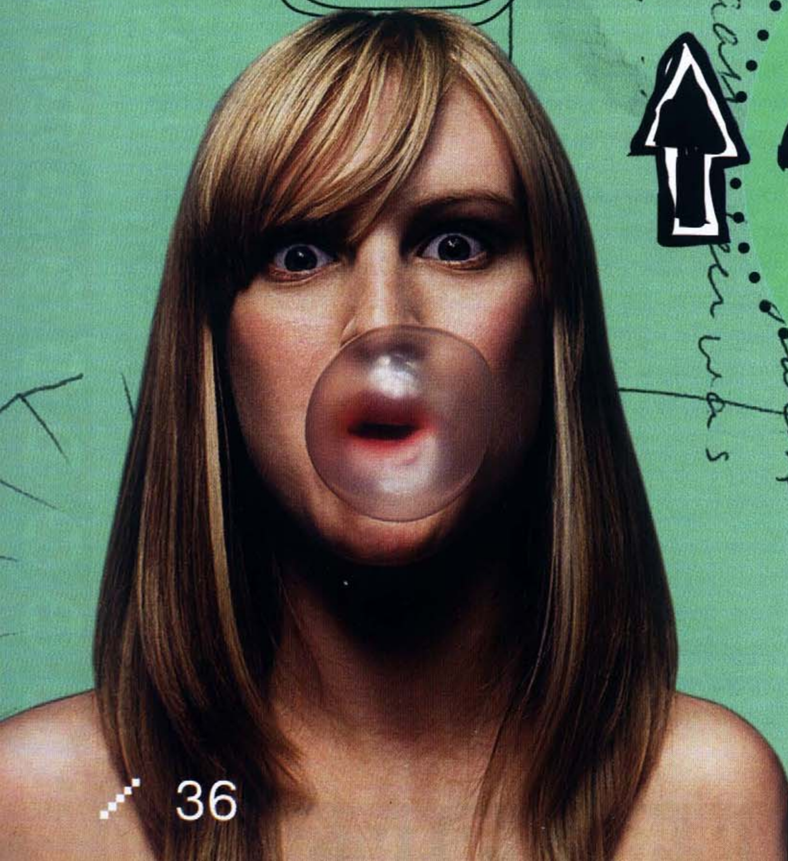
Jeigu tu ruošiesi užsiimti rimtesniais dalykais, pavyzdžiui, eksploitų kūrimu, tuomet iš pradžių išmok *C* ir Asemblerį.

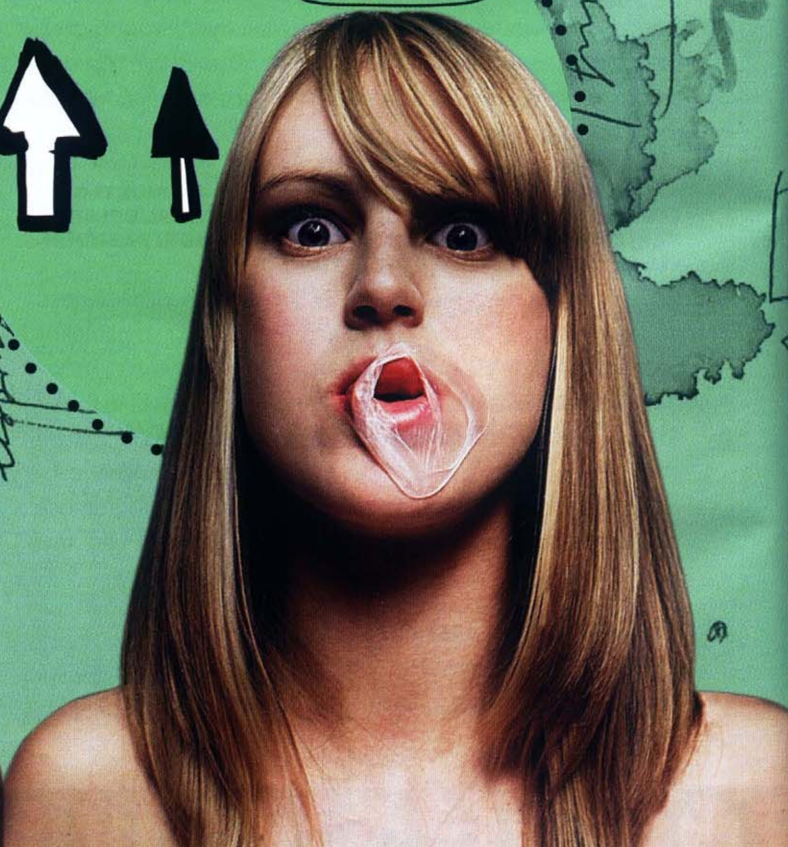
Šiaip ar taip, siūlyčiau anksčiau ar vėliau išstudijuoti *Perl*, kadangi tai universali kalba, kuri gali būti panaudota tiek *web* programavimui, tiek ir kaip paprasta skriptinė kalba kokių nors sisteminių UNIX ar *Windows* užduočių sprendimui.

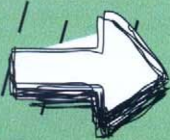
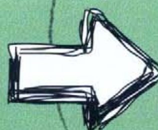
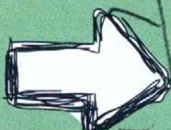
EKSPLOITŲ APŽVALGA

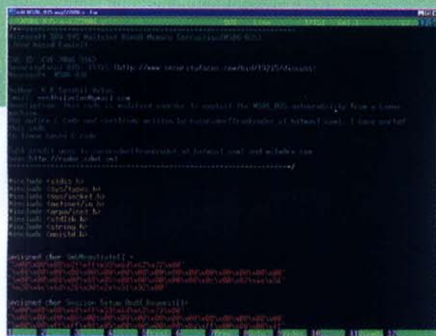




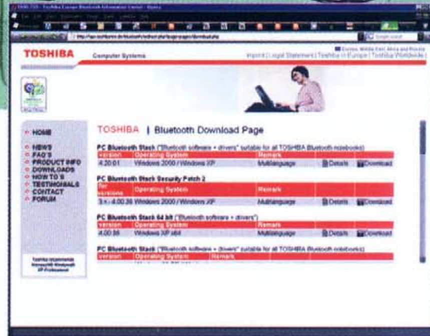






cocoruder'io sukurto eksploito išeities tekstas


Išorinis Google Earth svetainės vaizdas, kurioje ir toliau dalinama pažeidžiama programa


Iš čia galima parsisiųsti skylėtoms „Toshiba" tvarkyklėms skirtus pataisymus

„Microsoft Windows SMB": nuotolinis kodo įvykdymas

Brief

„File and Printer Service" servise buvo aptikta klaida, apie kurią raportavo iš karto 2 žmonės — *Gerardo Richarte* iš *Core Security Technologies* ir *Matthew Amdur* iš *VMWare*, taip pat NS *Focus* ir *Fortinet* tyrėjų grupės. Pasiuntus specialiu būdu sukonstruotą paketą bet koks neautorizuotas piktavalis gali sukelti esminį vidinių SRV.SYS tvarkyklės struktūrų suardymą, kas sukelia arba atsisakymą aptarnauti, arba valdymo užgrobimą nulinio žiedo lygyje. Visa tai suteikia neribotą valdžią sistemoje. Tokio triuškinančio paketo pavyzdys pateiktas eksploite, kurį sukūrė hakeris *cocoruder* ir kurį išpublikavo *Senthil Velan*. Išsamiau apie pažeidžiamumą rašoma „Microsoft" saugumo biuletenyje, užregistruotame numeriu MS06–063: *http://www.microsoft.com/technet/security/Bulletin/MS06-063.mspx*.

Targets

Pažeidžiamos praktiškai visos *Windows* sistemos: *w2k SP4*, *XP SP1/SP2*, *XP x86–64*, *Server 2003 / Server 2003 SP1 / Server 2003 x86-64 / Server 2003 IA64* (*Itanium*).

Exploit

Eksploito, sukeliančio atsisakymą aptarnauti (*DoS*, bet ne nuotolinį kodo įvykdymą), išeities tekstai pateikti *security–focus* serveryje: *http://downloads.securityfocus.com/vulnerabilities/exploits/MS06_035-aug222006.c*.

Solution

„Microsoft" jau išleido visoms savo sistemoms skirtus pataisymus, kuriuos galima parsisiųsti su *Windows Update*, tačiau mes neturime jokių garantijų, kad ši skylė užtaisyta pilnai. Taigi siekiant didesnio patikimumo rekomenduojama su ugniasiene uždaryti šias jungtis: UDP: 135, 137, 138 ir 445; TCP: 135, 139 ir 445.

„Google Earth": nuotolinis kodo įvykdymas

Brief

Pirmosiomis spalio dienomis tyrinėtojų kolektyvas *JAAScois Security Team* 2006 m. rugsėjo 13 dieną išleistoje programoje *Google Earth* (beta) aptiko milžinišką skylę. Pastaroji suteikdavo galimybę persiųsti shell–kodą ir taip užgrobti valdymą programą paleidusio vartotojo teisėmis. O daugelis vartotojų, kaip žinia, dirba administratoriaus vardu. *Google* programoje aptiktas tipiškas buferio perpildymas, paliktas *kml* ir *kmz* bylų apdorotuve: programa išskiria fiksuoto dydžio atminties bloką ir į jį kopijuoja priimtus duomenis, tačiau prieš tai pamiršta patikrinti faktišką šių duomenų dydį.

Target

Skylė slypi 4.0.2091 programos versijoje. Apie ankstesnes versijas kol kas nieko nežinoma. Paleidus programą kompiuteryje su įdiegta *Windows Vista* sistema ir su procesoriumi, kuris aparatiškai palaiko DEP (t.y. NX/XD bitus), sėkmingos atakos tikimybė dėl dalinai randomizuotos (atsitiktinės) adresų erdvės siekia 1/256, o likusiais atvejais pažeidžiama programa lūžta pranešdama apie kritišką klaidą.

Exploit

Eksploito išeities tekstą, kuris demonstruoja perpildymą, tačiau kuriame nėra shellkodo, galima parsisiųsti tiek iš *security–focus*, tiek ir iš paties *JAAScois Security Team* kolektyvo svetainės: *http://jaascois.com*.

Solution

Kadangi *Google* šiuo atveju elgiasi kaip strutis (t.y. slepia galvą smėlyje), rekomenduojama *Google Earth* (beta) nenaudoti tol, kol situacija pasikeis, t.y. išeis atnaujinta versija arba bent jau pataisymas.

„Toshiba Bluetooth stack": nuotolinis kodo įvykdymas

Brief

Kompanija „Toshiba" leidžia belaidžiams *Bluetooth* įrenginiams skirtas mikroschemas, kurias naudoja daugelis motininių plokščių ir kitos įrangos gamintojų. Ta pati „Toshiba" rašo šiai įrangai skirtas tvarkykles, kurios įgyvendina *Bluetooth* tinklo steką. 2006 m. spalio 11 dieną *David Maynor* iš „SecureWorks Inc." ir nepriklausomas tyrinėtojas *Jon Ellch* išpublikavo pranešimą apie skylę TOSRFBD.SYS tvarkyklėje. Ši skylė sukelia atminties suardymą su po to einančiu atsisakymu aptarnauti, t.y. sistemos persikrovimu arba mėlynuoju mirties ekranu (BSOD), o sėkmingai susiklosčius aplinkybėms — ir sistemos valdymo užgrobimu branduolio lygyje.

Targets

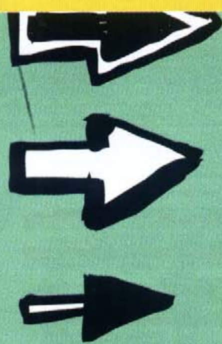
Pažeidžiamos visos tvarkyklių versijos nuo pat 3 iki 4.00.35 imtinai, taip pat ir *Toshiba Bluetooth Stack 4 SP2*. Šios tvarkyklės pateikiamos kartu su ASUS, „Dell", „Sony" ir kitų kompanijų leidžiama įranga. Nustatyti, ar konkrečiam įrenginiui gresia problemos, galima peržiūrėjus belaidžio įrenginio savybes pagal TOSRFBD.SYS tvarkyklę arba pagal gamintojo vardą („Toshiba").

Exploit

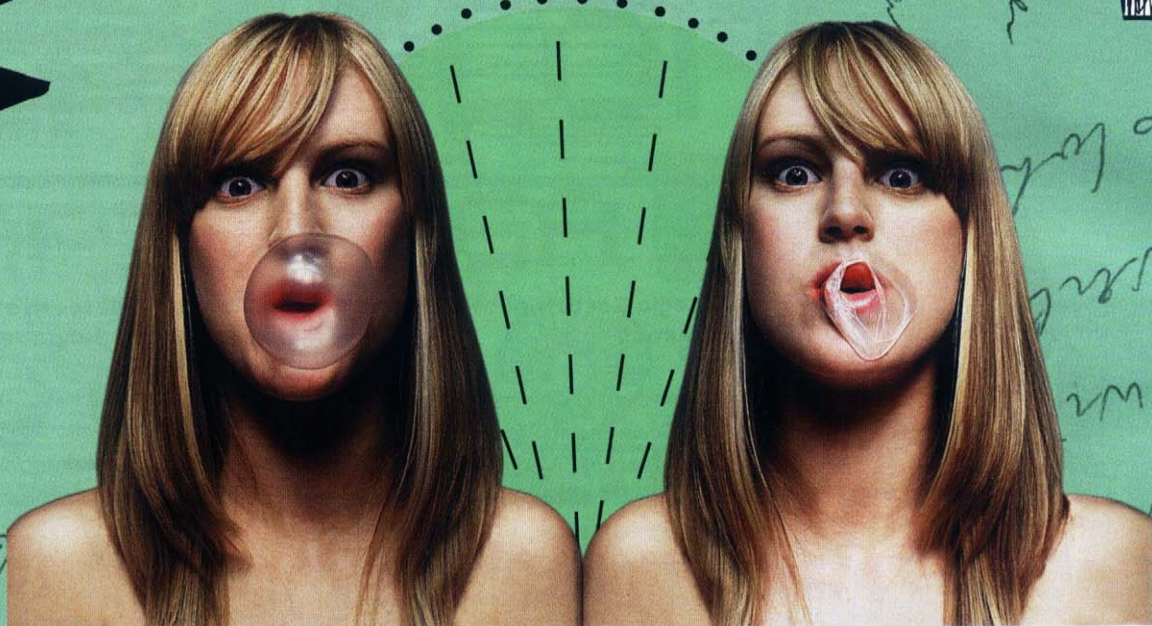
Norint atlikti ataką eksploito nereikia, pakanka kaip pridera prapinginti auką, ant jos užverčiant *L2CAP–echo* užklausų škvalą, ką galima atlikti su *linux* įrankiu *l2ping*. Šio tipo atakos ganėtinai populiarios ir vadinasi *BlueSmack*. Išsamiau apie tai paskaityti galima čia: *http://trifinite.org/trifinite_stuff_bluesmack.html*.

Solution

„Toshiba" išleido savo tvarkyklėms skirtus pataisymus, kuriuos parsisiųsti galima iš *http://aps.toshiba-tro.de/bluetooth/redirect.php?page=pages/download.php*.







Buferių perpildymas atšiauriomis „Vistos" sąlygomis

Brief

Turiu dvi naujienas: gerą ir blogą. Pradėsiu nuo geros. *Windows Vista/Server Longhorn* sistemose pilnai perrašytas tinklo stekas ir įdiegtas *IPv6*, kas padaryta labai keverziškai. Ankstesnėse betose buvo kartojamos praktiškai visos sename tinklo steke padarytos klaidos, kurias bandoma išlaižyti metų metus. Ir nors pagrindinės *Vista* skylės jau užlopytos, pats *IPv6* protokolas kartu su neištestuotu tinklo steku atrodo ganėtinai seksualiai ir atveria plačias perspektyvas pačioms įvairiausioms atakoms. Hakeriams tai tikras lobis. O dabar — bloga naujiena. „Microsoft" hakeriams priešpastatė ištisą priemonių kompleksą, kurios apsunkina shellkodo persiuntimą ir daugelį atakų, todėl prieš *Vistai* tampant dominuojančia sistema (o taip greičiausiai bus tik po metų–pusantrų), norintieji prie naujų sąlygų prisitaikyti kenkėjai turės atnaujinti savo ginklų arsenalą. Kas gi tai per apsauginiai mechanizmai ir ar juos galima apeiti? Būtent apie tai mes dabar ir pakalbėsim.

Intro

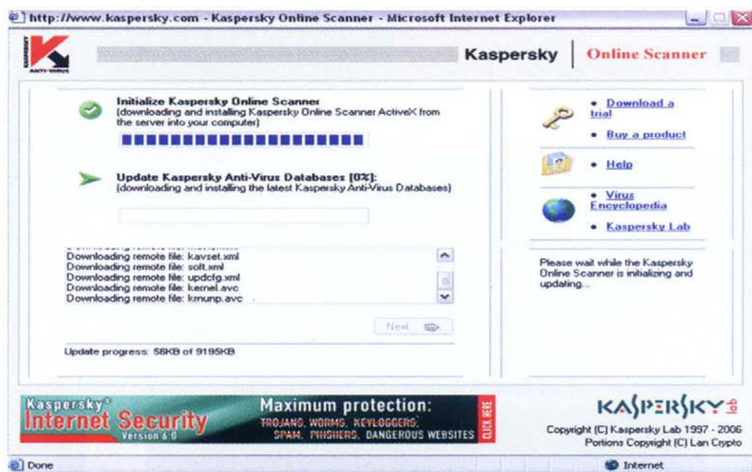
Pagrindinės gynybinės priemonės sumontuotos aplink persipildančius buferius, tačiau ši strategija pasmerkta žlugti, kadangi padidėjęs susidomėjimas šio tipo atakomis jau praėjo. Savo populiarumo piką pasiekusi 2005 metais, persipildančių buferių saulė ėmė leistis. Hakeriška mintis vietoje nestovi! Pamažu populiarėja tvarkyklių sinchronizacijos klaidas išnaudojančios atakos, kurių pavyzdžiais galima laikyti skyles *Intel Centrino* ir *Toshiba Bluetooth* tvarkyklėse, savo užgrobėjams suteikiančias branduolines nulinio žiedo privilegijas! Tačiau dabar vis dėlto sugrįžkime prie perpildomų buferių. Būtų kvaila pasiduoti be mūšio, juo labiau, kad „Microsoft'o" gynybą galima santykinai lengvai pralaužti.

DEP

Procesorių su aparatiniu DEP palaikymu dalis pasmerkta nepaliaujamam augimui. Ir nors *x86* platformose DEP pagal nutylėjimą aktyvuotas tik kai kuriems sisteminiams servisams, kadangi vis dar apstu programų, kurioms reikia vykdomo steko (tai ypatingai pasakytina pakuotojus, protektorius ir kitus apsauginius mechanizmus), gamintojai jau sureagavo į šią iniciatyvą. Naujosios versijos atributo PAGE_READ daugiau netraktuoja kaip PAGE_EXECUTABLE, todėl prieš kodo vykdymą *.text* sekcijai nepriklausančioje atminties srityje atributas PAGE_EXECUTABLE priskiriamas akivaizdžiai, kad programa taip galėtų dirbti su įjungtu DEP. Beje, tai privalomas „Microsoft" pateikiamas reikalavimas, jeigu nori pasipuošti *Windows Compatible* logotipu. Nesudėtinga prognozuoti, kad po keleto metų su DEP konfliktuojančių programų praktiškai visai neliks ir eiliniame *Vistai* skirtame pataisymų pakete (*Service Pack*) „Microsoft" paprasčiausiai galės politiką „DEP nesisteminėms programoms įjungtas pagal nutylėjimą" pakeisti į „DEP pagal nutylėjimą įjungtas visoms programoms". Pats DEP hakeriams gyvenimą apsunkina nesmarkiai ir yra lengvai apeinamas *retur–to–libc* tipo atakomis. Tačiau kombinuojant DEP su kitais apsauginiais mechanizmais jis pavirsta galingais šar-

Before	After	Explanation
buffer[1024]	Shellcode	
	"Success! ;) %d\n"	
	nothing meaningfulhere	
ret address of CalcAverage()	address of VirtualAlloc	address of VirtualAlloc
... rest of the stack ...	address of memcpy	exec memcpy after VirtualAlloc
	arbitrary address (191000h)	VirtualAlloc addess param
	shellcode+string size	VirtualAlloc size param
	MEM_COMMIT	VirtualAlloc alloctype param
	PAGE_EXECUTE_READWRITE	VirtualAlloc protection param
	arbitrary address (191000h)	Exec our shellcode after memcpy
	arbitrary address (191000h)	_dest param of memcpy
	address of buffer[0]	_src param of memcpy
	shellcode+string size	size param of memcpy
	... rest of the stack ...	

Steko paruošimas atakai prieš DEP



64 bitų Windows versijose „Microsoft" sukonfigūravo draudimą modifikuoti branduolį, dėl ko antivirusų egzistavimas tiesiog neįmanomas, todėl jie su šios sistemos atėjimu yra pasmerkti išnykti. Išliks tik autonominiai skeneriai

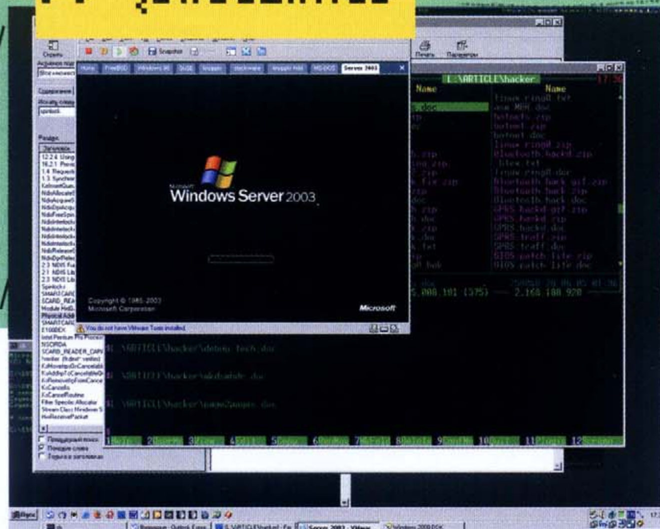
vais, kurių egzistavimą nori nenori tenka įvertinti, kaip kad tenka įvertinti ir tai, jog šie šarvai pramušami su kumuliatyviniais sviediniais, kuriuos rinkoje populiarina ta pati „Microsoft" .NET platformos, pagrįstos interpretuojama kalba *C#*, pavidalu. Nepaisant to, kad palyginus su *C*, naujoji *C#* kur kas mažiau linkusi į buferio perpildymo klaidas, apsauginės DEP priemonės jai negalioja, kadangi procesoriaus požiūriu interpretuojamas kodas — tai duomenys, kuriems PAGE_EXECUTABLE atributas nereikalingas. Iš tikrųjų *C#* nėra visiškai interpretuojama, o kompiliuojama į atmintį, beje, sukompiliuotas kodas įkeliamas į atminties sritį, į kurią galima tiek rašyti, tiek ir vykdyti. Taigi procesorių su DEP galimybe populiarėjimą kompensuoja pergalinga .NET'o eisena, su kuria patogu rašyti sąsają, tačiau realizuoti visą programą — ačiū, ne. Visų pirma, *C#* kur kas labiau artimesnė *Visual Basic'ui*, negu *C*, o koks *Basic'o* našumas? Antra, su *C/C++* sukurta daugybė bibliotekų, kurių niekas nesiruošia perrašinėti su .NET, todėl artimiausius 3–5 metus didžioji programų dalis bus kuriama hibridiniu principu — *C/C++* plius *C#*, kas leis per *C#* eksploatuoti *C/C++* būdingas perpildymo klaidas! Jeigu hakerių aktyvumas ir sumažės, tai nesmarkiai.

Randas

Klasikiniame atakos prieš persipildančius buferius scenarijuje grįžimo iš funkcijos adresas pakeičiamas į mašininės komandos *jmp esp* (opkodas *FFh E4h*) adresą, kuris rūno kažkur operatyvinėje atmintyje, o panašių komandų ten per akis. Tokios dviejų baitų sekos plačiai sutinkamos tiek sisteminėse bibliotekose, tiek ir pačiose atakuojamose programose. *jmp esp* valdymą perduoda į steko viršūnę, kurioje yra perpildytas buferis su shell–kodu, ir viskas eina pagal seną gerą planą, išaugusį karštos pietų saulės spinduliuose. Tačiau su įjungtu DEP toks planas negali nė uodegos pajudinti, kadangi komandų vykdymas steke kategoriškai draudžiamas, dėl ko tenka atlikinėti galybę papildomų veiksmų, kad pašalintum šiuos apgailėtinus nemalonumus. Paprasčiausia, ką galima padaryti — į steką įkelti API funkcijos *VirtualProtect* adresą, kuri leidžia valdyti priėjimo prie atminties atributus, o paskui ją — ir API funkcijos *MoveMemory* adresą, kuri shellkodą iš steko kopijuoja į atminties sritį, jau apdorotą su funkcija *VirtualProtect*, kuriai ši priskyrė atributą „vykdomas". Telieka valdymą perduoti į šią sritį, tam į steką įkeliamas naujos shell–kodo dislokacijos adresas, o tada viskas atsiduria mūsų rankose.

Kaip matome, nepriklausomai nuo DEP būsenos mes turime žinoti atakuojamos aukos adresų erdvės turinį, kad atmintyje surastume *jmp esp* instrukciją arba API funkcijų adresus. XP ir *Server 2003* sistemose tai buvo galima padaryti be jokių nesklandumų, kadangi ir pati vykdoma byla, ir sisteminės bibliotekos visada užkraunamos tais pačiais adresais. Žinoma, šie adresai nesiskiria tik vienos konkrečios *Windows* versijos rėmuose ir jie gali keistis su kiekvienu pataisymų paketu, kas atakuojantįjį priverčia versiją nustatyti arba netiesiogiai būdu, arba tiesiog veikti aklai. Jeigu jam pasiseks — jis kaifuos, priešingu atveju aukos sistema nulūš su kritinės klaidos pranešimu, o kartu su tuo mūsų laukia vargai vargeliai. Pastoviu ir nepriklausomu nuo versijų išlieka tik bazinis pačios pažeidžiamiausios programos užkrovimo adresas, bet čia nelabai yra už ko užsikabinti, kadangi keičiantis versijai keičiasi ir jos turinys. Noriu pasakyti, kad parašyti universalią atakuojančią programą, kuri gali sudoroti visas sistemas, ne taip jau paprasta, o bendru atveju — iš viso neįmanoma, tačiau tai vis tiek neatima malonumo. Nors *Windows* versijų skaičius (kartu su pažeidžiamos programos versijomis) ir didelis, tačiau jis vis dėlto baigtinis. Jeigu atkakliai pulsi auką, ji anksčiau ar vėliau pasiduos, shellkodas gaus valdymą, ir visi bus labai laimingi. Na, galbūt beveik visi.

Kas pasikeitė *Vista* sistemoje? Sisteminės bibliotekos dabar kraunamos vienu iš 256 galimų bazinių adresų, kuris parenkamas atsitiktiniu būdu. Vykdomų bylų antraštėje atsirado specialus bitas, kuris parodo, ar programa turi krautis fiksuotu, ar atsitiktinai parinktu adresu. Tas pats pasakytina ir apie nesistemines dinamines bibliotekas. Tai reiškia, kad šiuo metu realiai atsitiktinius adresus naudoja tik sisteminės



Vista pagrįsta šiek tiek „patobulintu" Server 2003 SP1 branduoliu



AMD Athlon procesorius su aparatiniu DEP palaikymu

bibliotekos ir kartu su standartiniu *Vista* komplektu pateikiamos programos. Visos anksčiau parašytos programos kraunasi vienu ir tuo pačiu adresu, ir taip bus dar ilgai, kadangi trečiųjų šalių gamintojai ypač šaltai reaguoja į naująją „Microsoft" iniciatyvą. Ir net kai atsiras randomizacijos vėliavėlę pripažįstantys linkeriai, tai dar nereiškia, kad visi paskubės juo pasinaudoti. Priežastis čia slypi tame, kad krovimasis laisvai parinktu adresu reikalauja perkeliamų elementų lentelės, padidėja operatyvinės atminties kiekio poreikis (ypač jeigu paleidžiama keletas programos kopijų) ir palengvina laužimą, kadangi egzistuojantys pakuotuvai/protektoriai nepalaiko randomizacijos ir bylą išpakuoja pagal fiksuotus adresus. Iš čia išplaukia, kad dalis pažeidžiamos programos adresų erdvės, kuri susijusi su vykdoma byla ir jos asmeninėmis dinaminėmis bibliotekomis, kaip ir anksčiau lieka nuspėjama. O tai atakuojančiajam leidžia valdymą per *jmp esp* laisvai perdavinėti į shell–kodą, taip pat iškviesti bet kokias pažeidžiamoje programoje aprašytas arba joje importuojamas funkcijas, nors konkrečiai paimtos programos importo lentelėje jos iš viso gali ir nebūti. Iš tikrųjų situacija praktiškai nepasikeitė. Sėkmingos atakos tikimybė (įvertinus *Windows* versijos heap'ą) ir anksčiau nesiekė 100 %, tuo tarpu dabar ji sumažėjo maždaug 256 kartais. Ir visa tai jie dar drįsta vadinti patikima apsauga! Na na... Čia tas, kas labai nori, savo tikrai pasieks. Jeigu hakeris atkakliai bandys, anksčiau ar vėliau jis atspės pagrindinį KERNEL32. DLL adresą, o šioje bibliotekoje jis ras visas jam reikalingas funkcijas, po ko auka kris. Tiksliau šnekant, viskas bus atvirkščiai — tuomet bus užgrobtas nutolusios mašinos valdymas, o visais kitais atvejais ji lūš. Administratorių užknis iš naujo paleidinėti serverį (arba darbo stotį), nes jis greičiausiai nesupras, ar jį atakuoja, ar pas jį kažkas klaidingai veikia (pavyzdžiui, atmintis). Tiesa, turėdamas įtarimų dėl atakos, jis galės greitai parsisiųsti visus atnaujinimus (su sąlyga, kad jie yra) ir užkamšyti skyles. Tačiau nuolat atakuojant kompiuteris lūžinės taip dažnai, kad nepavyks nieko parsisiųsti! Bet lūžimai nėra gerai. Kam pritraukti papildomą dėmesį? Norint išvengti pranešimų apie kritines klaidas, būtina perrašyti rodyklę į einamą struktūrinių išimčių apdorotuvą, su kuriuo susijusi dar viena „Microsoft" gynybos iniciatyva — *Vistoje* jis perkeltas iš lengvai perrašomo steko į tik skaitymui prieinamą *.pdata* sekciją. Visa tai pasakytina tik apie statinius struktūrinių išimčių apdorotuvus, kurių adresas žinomas dar kompiliavimo stadijoje. Tai galioja su paprastomis *C* programomis, tačiau *C++* atveju ganėtinai daug apdorotuvų konfigūruojama dinamiškai. Be to, apdorotuvų konfigūravimu užsiima kompiliatorius, o visi egzistuojantys kompiliatoriai rodykles į apdorotuvus įkuria steke! Taigi *Vista* atsiradimas pats savaime nieko nekeičia. Iš pradžių reikia sulaukti bent jau atnaujintų kompiliatorių versijų, o iki tol struktūrinių išimčių apdorotuvus galima drąsiai perrašinėti ir perkonfigūruoti pagal savo poreikius. Tiesa, pradedant *Server 2003 OS*, sistema atlieka papildomą patikrinimą, kuris užkerta kelią apdorotuvo kodo įkūrimui steke. Bet... čia galima pakišti vieno iš pažeidžiamos programos apdorotuvų adresą, kuris neužbaigtų programos darbo ir į ekraną neišmestų jokių klaidų ar pranešimų, o vienaip ar kitaip apdorojęs išimtį įprastiniu režimu pratęstų darbą. Daugeliu atvejų tam pakanka iš karto peršokti į apdorotuvo vidurį, kur nors arčiau API funkcijos *Continue*, o tada galima drąsiai atakuoti nepersipildantį buferį, vieną po kito perrenkant visus įmanomus variantus.



> Microsoft's way

Specialistai rekomenduoja ICG KOMPIUTERIAI

Ką galima nusipirkti už 599 Lt?

GALINGĄ NEŠIOJAMĄJĮ KOMPIUTERĮ SU OMNI CONNECT IR SKYSTŲJŲ KRISTALŲ TELEVIZORIŲ!







Mėnesinis mokestis už neribotą mobilųji internetą
bei nešiojamąjį kompiuterį 179 LT/mėn. Sutarties terminas 36 mėn.
Sutarties mokestis 599,-

NEĮTIKĖTINAS SPRENDIMAS - PIRKITE NEŠIOJAMĄJĮ KOMPIUTERĮ SU NERIBOTU MOBILIUOJU INTERNETU OMNI CONNECT IR LG SKYSTŲJŲ KRISTALŲ TELEVIZORIŲ GAUSITE DOVANŲ.

SPECIALIAI JUMS SIŪLOME IŠSIRINKTI VIENĄ IŠ TRIJŲ AKCIJOS NEŠIOJAMŲJŲ KOMPIUTERIŲ:



DOVANA



OMNI CONNECT

599,-

PATIKIMUMAS

TOSHIBA SATELITE L30-134

EKRANAS 15,4", PROCESORIUS INTEL CELERON 410 1.6GHZ, ATMINTINĖ 512MB DDR2, KIETASIS DISKAS 60GB, VAIZDO PLOKŠTĖ ATI X200 256MB, DVD ĮRAŠANTIS ĮRENGINYS, BELAIDIS INTERNETAS, MICROSOFT WINDOWS HOME. BATERIJA 6CELL, DIRBA IKI 3 VALANDŲ, SVORIS 2.7KG, TARPTAUTINĖ GARANTIJA 24MĖN.



DOVANA



OMNI CONNECT

599,-

MOBILUMAS

ASUS AZ99H

14'1" YPAČ RYŠKUS EKRANAS, PROCESORIUS INTEL YONAH 420 1.6GHZ, ATMINTINĖ 512MB DDR2, KIETASIS DISKAS 60GB VAIZDO PL. INTEL 224MB, DVD +/-RW ĮRENGINYS, BELAIDIS INTERNETAS ENERGIJOS TAUPYMO SISTEMA POWER 4GEAR, JUNGTYS: USB2.0 5VNT VIDEO KAMERŲ 1394, FOTO KORTELIŲ, TV-OUT. BATERIJA 6CELL DIRBA IKI 3VALANDŲ. SVORIS TIK 2.4 KG TARPTAUTINĖ GARANTIJA 24 MĖN. ASUS KREPŠYS IR PELĖ DOVANŲ.



DOVANA



OMNI CONNECT

599,-

STILINGUMAS IR PRAMOGOS

HP PAVILION DV6103

NAUJOS KARTOS DIZAINO, "STIKLINIS" YPAČ RYŠKUS 15,4" EKRANAS PROCESORIUS SEMPRON MOBILE 1.8GHZ ATMINTINĖ 512MB DDR2 KIETASIS DISKAS 80GB SATA VAIZDO PL. GEFORCE 6150 128MB BELAIDIS INTERNETAS DISTANCINIS VALDYMAS ALTEC LANSING KOLONĖLĖS TV OUT JUNGTIS MICROSOFT WINDOWS HOME OFISAS WORKS 8.0

OMNI CONNECT
PARTNERIS

Tik ICG ir ICG Partnerių salonuose
*Daugiau informacijos WWW.ICG.LT TEL.: 8~700~55021

ICG KOMPIUTERIAI

Ne visos svetainės vienodai naudingos



PASLĖPTA „CRACK" SVETAINIŲ ŽALA

VISI SUSIDURIA SU TOKIU REIŠKINIU, KAIP TIKSINTIS GODŽIOS PROGRAMOS LAIKRODUKAS, SKAIČIUOJANTIS JOS GYVENIMĄ. KAI ŽMOGUS TURI MAŽAI PATIRTIES, JIS MUŠA ŠAMANO BŪGNĄ IR SUKA RATUS APLINK KOMPIUTERĮ, MELSDAMAS SHAREWARE IR TRIALO DIEVŲ ATLAIDUMO. BET TU NE PĖSČIAS, TODĖL IŠ KARTO EINI Į CRACK SVETAINĘ IEŠKOTI VAISTUKŲ NUO GODUMO. LEISK PAPASAKOTI TAU APIE NEGERUS DALYKUS, KURIE GALI TAU NUTIKTI.

Trindamas godžias rankas tu žibančiomis akimis brauniesi prie slaptojo kreko. Savo kelyje nušluoji krūvą flash'o ir iššokančių (*pop-up*) langų su kvietimais nemokamai pažiūrėti pornografijos, perklausyti tūkstančius gigabaitų *mp3* ir padidinti savo penį su 15% nuolaida. Įveikdamas šias kliūtis, tu atsargiai parsisiunti tau reikalingą mažytę bylą, patikrini ją savo šviežiai atnaujintu antivirusu ir ramia širdimi paleidi programą. Valio! Programa išgijo nuo patologiško kūrėjų godumo ir yra pasiruošusi ištikimai tarnauti tavo fronte. Džiūgaudamas ir velniškai juokdamasis tu atsijungi nuo tinklo... Tuo tarpu sistemos gelmėse prasidėjo kruopštus darbas — dešimtys mažyčių programų lyg skruzdėlės kapstosi sisteminių *dll* bibliotekų viduriuose, įsiskverbia į tavo naršyklę ir pradeda stebėti susijungimą su tinklu, pasirengusios visą gautą informaciją išsiųsti savo slaptam šeimininkui. „Kas per nesąmonės, juk aš naudoju antivirusą ir neatidarinėjau nieko nereikalingo!" — stebiesi tu. O viskas todėl, kad geri dėdės kartu su vaistukais tau įbruko krūvą kilobaitų šlamšto, apeinančio kompiuterio apsaugas.

Bendras užkrėtimo mechanizmas paprastas: tu užeini į „užkrėstą" svetainę. Dėl naršyklės skylių į tavo sistemą užkraunamas, o po to ir paleidžiamas Shell-kodas. Trojanas toks nedidelis, kad net prisijungęs per modemą tu nieko nepajausi. Shell-kodas paleidžia aplinką, o po to vyksta patys įdomiausi dalykai: atidaroma jungtis, pradedamas siuntinėti spamas arba inicijuojama kokio nors resurso *DoS* ataka.

Su tokiais virusais tu gali susidurti kur tik nori, tačiau ypatingai daug jų galima rasti krekų svetainėse. Nieko čia nuostabaus, juk, kaip žinia, nemokamas sūris būna tik pelėkautuose. Taigi, mano mielas skaitytojau, norėdamas apsaugoti tave, aš ir ėmiausi šios sunkios ir mano sistemai kenksmingos apžvalgos. Pradė-







› Nuorodos į svetaines, kuriose knibždėte knibžda virusų :)

jau nuo to, kad įdiegiau plikas langines (XP+SP1, jokių pataisymų paketų), o visus sisteminius nustatymus palikau pagal nutylėjimą — *Java* įjungta, *ActiveX* elementai — taip pat. Tada sustabdžiau antiviruso ir ugniasienės darbą (atitinkamai AVP ir *Outpost*). Turiu prisipažinti, kad šiek tiek nervinausi, kadangi man teko su tokia vargana sistema išplaukti į laukines interneto erdves, tačiau rezultatai pranoko visus mano lūkesčius.

Visų pirma, aš užsukau į *astalavista.box.sk* — populiariausią *crack* svetainių paieškos sistemą. Derindamas malonumą su nauda, užsimaniau surasti programai *Wav Joiner* skirtus vaistukus. Šis įrankis apjungia kelias *wav* bylas į vieną, tačiau už jį prašo 30–ies dolerių. Į paieškos lauką įvedęs programos pavadinimą, gavau sąrašą su 6 svetainėmis. Pirmoji iš jų vadinosi *cracks.am*. Ignoruodamas iššokančius ir *flash* langus, aš prasibroviau iki nuorodos į kreką. Tačiau mano kelionės metu sistemoje vyko kažkokios anomalijos: naršyklė nuolat pakibdavo, užduočių juostoje porą kartų sekundei pasirodydavo juodas konsolės langas. Tai rodė, kad kažkoks užkratas spėjo prasibrauti į mano neužlopytą sistemą. Paleidęs parsisiųstus vaistukus aš gavau pranešimą apie programos versijos nesuderinamumą. Keista, tačiau kreko aprašyme paminėta būtent ta versija, kuri buvo įdiegta mano kompiuteryje. Vėliau paaiškėjo, kad krekas — tai paprasčiausia klastotė, į laisvę paleidžianti *RPC–DoS* trojaną. Nuo pseudokreko paleidimo kas pusę valandos internetas pradėdavo stabdyti, o po poros priverstinių perkrovimų sistema puolė į komą (tuo metu aš pradėjau karštligiškai štampuoti screenshot'us ir išsaugoti viską, kas papuolė po ranka). Po poros meditacijos minučių langinės nulūžo su BSOD. Akivaizdu, kad dėl to buvo kalti tinklą skenuojantys ir neužlopytus kompiuterius užkrečiantys skriptai. Galbūt tai buvo *Net–Worm.Win32.Francette.a* arba *Raleca* (šį užkratą po to surado mano antivirusas).

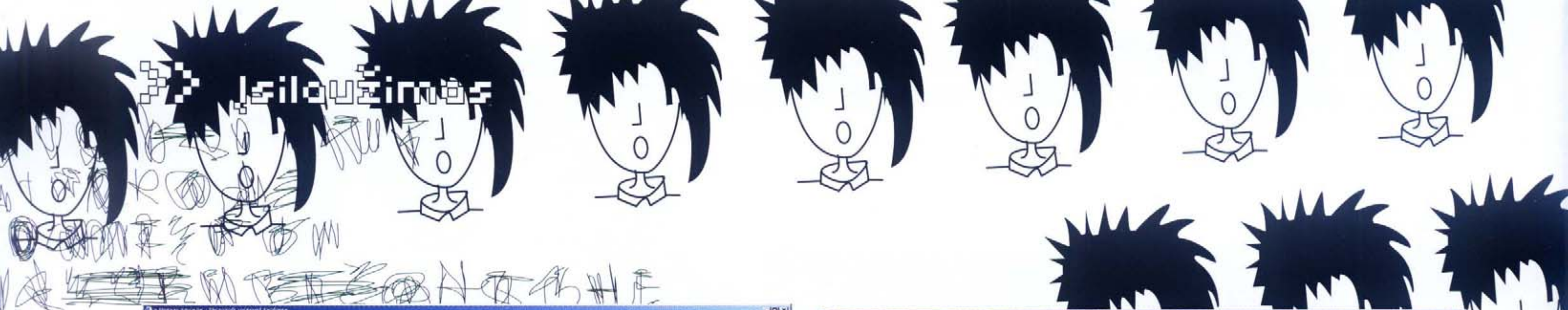
Aiškinamės

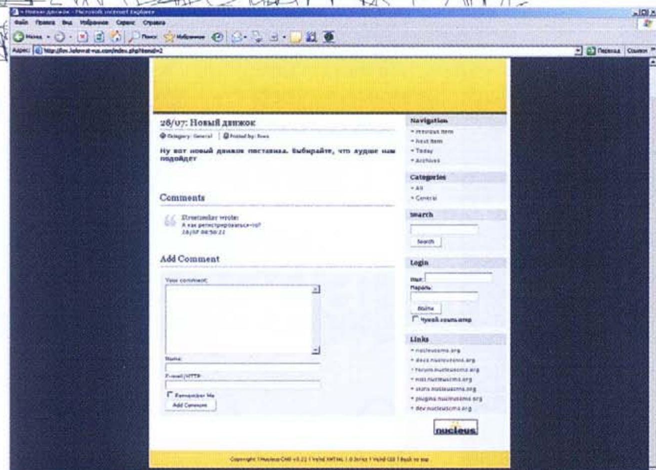
Man nieko neliko, kaip tik užsikrauti *Safe Mode* ir su AVP patikrinti sistemą. Skenavimas parodė, kad mano mašinoje apsigyveno net 3 skirtingi virusai (ir tai užėjus į viso labo vieną resursą)! Vis dėlto intuicija man sakė, kad kompiuteryje slepiasi dar kažkas. Ir aš buvau teisus. Perėjęs į sisteminį langinių

SAUGAUS GYVENIMO PAGRINDAI

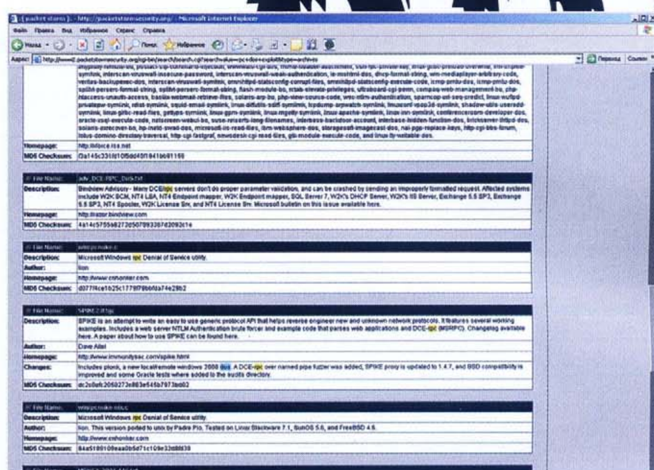
JEIGU TU NEGALI GYVENTI BE „CRACK" RESURSŲ, TUOMET BŪTINAI LAIKYKIS ŠIŲ REKOMENDACIJŲ.

1. Navigacijai po „haliavnas" svetaines nenaudok IE. Rekomenduoju pas save įdiegti paskutinę FireFox versiją, kurioje kur kas mažiau klaidų. O iš viso geriausia crack portalus naršyti su konsoliniu lynx.
2. Jeigu naudoji WinXP, tuomet būtinai pas save įdiek SP2 ir visus papildomus pataisymus.
3. Įsidiek ugniasienę (čia jau skonio reikalas, tačiau pageidautina, kad joje būtų integruotas skriptų tikrinimo mechanizmas) ir antivirusą.
4. Atjunk Java (nors vargu ar tu su tuo sutiksi — tokiu atveju daugelis šiuolaikinių web puslapių atrodys ganėtinai bjauriai, smarkiai turėtų pasunkėti navigacija) ir nepasirašytus ActiveX elementus. Taip pat atjunk sausainukų priėmimą iš visų resursų (po to rankiniu būdu galėsi surašyti tas svetaines, kurioms tai leidžiama).
5. Reguliariai tikrink hosts bylą, ar joje nėra pašalinių nuorodų, nes pagal nutylėjimą ten turėtų būti tik viena eilutė: „127.0.0.1 localhost" (be kabučių).
6. Pasidaryk sistemos ir tinkle naudojamų programų atvaizdus, o tada kartą per savaitę sutikrink jas su kontroliniais atvaizdais. Jeigu žvėris ir įsibraus, tu nesunkiai galėsi susekti, kada ir kaip tai įvyko. Manau, nereikia priminti, kad didžiausios rizikos kategorijai visų pirma priskiriamos porno–warez–crack svetainės. Iš esmės, šių svetainių savininkų ideologiją galima suprasti, kadangi jie uždirba iš nedorybių ir tuo pačiu už šias nedorybes baudžia.





› Štai tokiose svetainėse ir landžioje visokie žvėrys



› Čia pateiktų išeities tekstų užtektų keletui dešimčių virusų

katalogą (*c:\windows\system32*), aš visas bylas surūšiavau pagal sukūrimo datą. Paaiškėjo, kad sistemoje gyvena kažkokie *system32.dll* ir *system32.com*, sukurti kelionių po *cracks.am* metu. Iš karto ėmiausi stebėti einamus procesus, tačiau paaiškėjo, kad šis sutvėrimas (arba koks nors kitas trojanas) taip sukonfigūravo lokalią politiką, kad aš negalėjau paleisti *Task Manager*. Žinoma, aš tokią politiką greitai pakeičiau, tačiau paaiškėjo, kad antivirusas pastebi toli gražu ne visus trojanus.

Kiti resursai, kuriuose apsilankiau, buvo *crackportal.com*, *serialsite.com*, *subserials.net*, *warezz.nm.ru* ir *crackers.org* (iš eilės). Visuose portaluose atsidarinėjo iššokantys langai ir užsikrovinėjo trojanai. Vis dėlto ir pelenuose galima rasti žvilgančio aukso: vienintelis *crackers.org* man pateikė švarų kreką, kuris be jokių papildomų pasekmių nulaužė man reikalingą programą.

Norisi papasakoti apie *crackportal.com*, tiksliau šnekant, apie vieną kenksmingą iššokantį langą, kuris atsidaro pasirinkus kreką. Panaudojant naršyklės pažeidžiamumą į sistemą parsiunčiamas „paveiksliukas" *pic10.jpg*, kuris iš tiesų yra vykdoma byla ir kuris pakeičia *Windows Media Player*. Po to parsiunčiamos programos *web.exe* ir *classload.jar*, paleidžiamas apletas, kuris nustato langinių buvimo vietą (*GetWindowsDirectory()*), ten įkelia *web.exe* ir jį paleidžia. Tiesiog stebuklingai sistemoje atsiranda trojanas *Trojan.Win32.Spooner.f*. Šis, savo ruožtu, paskui save parvelka *Trojan–Downloader.Win32.Small.apf*. Kitaip tariant, prasideda konkreti betvarkė, kuri pasibaigia tuo, kad kompiuteryje atsiduria *Trojan–Spy.Win32.Banker.jk*, *Trojan–Proxy.Win32.Small.bh*, *Backdoor.Win32.Zins.c*, *Trojan–Dropper.Win32.Small.vn*, *Trojan–Dropper.Win32.Small.wp*, *Trojan–Downloader.Win32.Agent.lv* ir *Backdoor.Win32.Jeemp.c*. Kaip smagu, tiesa? Be to, modifikuojama *hosts* byla (*%systemroot%\system32\drivers\etc*), kurioje blokuojami Kasperskio, *McAfee* ir *Symantec* adresai. Maža to, kaip aš pastebėjau, sugeneruojama suklastota *html* byla, kuri įkurdinama ant darbastalio ir kuri vartotojui praneša apie tai, kad jo sistemoje yra mažiausiai 3 pavojingi virusai, todėl vartotojui siūloma užeiti adresu *topantivirus.biz*, iš kur galima parsisiųsti gerą antivirusą.

Flash filmukai, kurie pastoviai rodomi tiek *crack*, tiek ir kituose resursuose, taip pat gali pasigirti įvairių užkratų gausa. Prisimink *adware* trojaną, kuris buvo pateikiamas *MySpace'e*. Flashas, reklamavęs užsienietišką svetainę *deckoutyourdeck.com*, išnaudojo su *.*wmf* susijusią langinių skylę. Oi, kiek buvo triukšmo! Nors iš esmės šis virusas nieko neištrindavo, tačiau užknisdavo negyvai — nuolat išmesdavo krūvą iššokančių langų su daugybe reklaminių antraščių plius stebėdavo interneto naršymą. Tada ši bjaurybė užkrėtė apie 2 milijonus mašinų, padarė žalos už 3 milijonus dolerių. Aš jį pastebėjau *cracks.am* svetainėje (per *flash* filmuką man lengvai buvo įkeltas kirminas *Net–Worm.Win32.Francette.a*).

Po mano ilgo eksperimento paaiškėjo neginčijama tiesa: kuo mažesnė svetainė, tuo didesnė tikimybė, kad jis pilnas kirminų nuo pat *<html>* tago pradžios iki paskutinio pikselio ant jo snukelio. Pasirausęs visoje šitoje pamazgų duobėje, aš iš jos išlindau besipuikuodamas 16–kos rūšių bjaurybėmis. Tarp jų buvo mažai žinomi *JS.Scob.Trojan*, *JS.Scob.Trojan.b*, *Bofra*, *Troj/Borobt–Gen*, *Trojan-Clicker.Win32.Small.h* (šį užkratą kažkas modifikavo, kadangi originalas vesdavo į *www.sex.de*, o pastarasis rodė jau į kitą svetainę) ir dar krūva mažų kirminiukų. Vienas jų man suteikė nemažai džiaugsmo. Mažasis išsigimėlis bandė savo kūnelį paslėpti šifruodamasis XOR'u :)

Tom Clancy's RAINBOW SIX VEGAS

JAVA ŽAIDIMAS

LG: c1300. **Motorola:** c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 6020, 6030, 6060, 6100, 6230, 6230i, 6600, 6610, 6670, 6680, 7210, 7250, 7260, 7610, n70. **Samsung:** d500, d500e, d600, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600.

J5410181304

1. **Rašyk žinutę su kodu:** Pvz.: J5410181304, draugui: J5410181304 370699XXXXX
2. **Jei priklausai OMNITEL ar BITĖ, siųsk numeriu: 1390**
Jei priklausai TELE2, siųsk numeriu: 1399

WAP 10 LT

ANIMACIJA



W5410181405 W5410181383 W5410181401 W5410181404

1. **Rašyk žinutę su kodu:** Pvz.: W5410181202, draugui: W5410181202 370699XXXXX
2. **Siųsk numeriu: 1390**

WAP/GPRS 2 Lt

NOKIA: 2600, 2650, 3100, 3108, 3120, 3128, 3200, 3220, 3230, 3510i, 3530, 3660, 5100, 5140, 6020, 6021, 6030, 6101, 6108, 6170, 6220, 6230, 6260, 6600, 6610i, 6620, 6630, 6670, 6680, 6681,6810, 6820, 6822, 7200, 7250, 7250i, 7270, 7610, 7650, 9300, 9500, N-Gage, N-GageQD, **SIEMENS:** A60, A62, A65, A75, Ax75, C62, CF75, CL75, CX65, CX70, CX75, CFX65, CXT65, E700, E800, M55, M75, MC60, S65, SF65, SK65, SP65, ST55, Sl60, V500, V560, X100, X120, X600, X640, **MOTOROLA:** C350, **SONY-ERICSSON:** T610, T630

SPALVOTI PAVEIKSLIUKAI

F5410182665 F5410181189 F5410184106 F5410184106 F5410182691 F5410183943

F5410182709 F5410182761 F5410182686 F5410184109

VAKAR BUVO LINKSMA... F5410184115

F5410182770 F5410181346 F5410182698 F5410184045

F5410181198 F5410181403 F5410181314 F5410184000 F5410184060 F5410184114

F5410181968 F5410181476 F5410184112 F5410184118 F5410182692 F5410184119

1. **Rašyk žinutę su kodu:** Pvz.: F5410184115, draugui: F5410184115 370699XXXXX
2. **Siųsk numeriu: 1390**

WAP/GPRS 2 Lt

NOKIA, SIEMENS: su WAP nustatymais, **SAMSUNG:** D100, E100, E700, E710, P100, P400, P510, S100, S500, T500, X400, X450, D700, V100, P700, **MOTOROLA:** C350, C370, C450, C550, E380, C650, **SONY-ERICSSON:** 300, T68, T302, T306, T310, T312, T316, T230, Z200, Z208, Z500, Z600, Z608, K700c, K700i, Z1010

PAVEIKSLIUKAI SU TEKSTU



T5410181084 T5410181081 T5410181086 T5410181080

T5410181089 T5410181087 T5410181079 T5410181085

1. **Rašyk žinutę su kodu:** Pvz.: T5410181042 TEKSTAS 2. **Siųsk numeriu: 1390**

Ši paslauga tinka tokiems patiems telefonų modeliams, kaip ir spalvotų paveikslėlių

WAP/GPRS 2 Lt

MELODIJŲ TOP 20

1	69 DANGUJE - Gyvenu	5410182387
2	DIMA BILAN - Never Let You Go	5410182294
3	NL - Užknisa tavo skambučiai	5410182369
4	ЮРИЙ ШАТУНОВ - Белые розы	5410182363
5	КУКЛЫ НА ПРОКАТ - Капали слезы	5410182396
6	АЙДАМИР МУГУ - Чёрные глаза	5410182331
7	BUMER-2	5410182234
8	YVA - Katyčių daina	5410182372
9	NL - Ruri Ruri	5410182366
10	ANDRIUS RIMIŠKIS - Kam tu man	5410182383
11	NL - R-1	5410182365
12	SNIEGĖ IR KARINA - Ten	5410182359
13	MAMA ROCK'N'ROLL - Merguželė	5410182324
14	BUMER 2 - Осень	5410182349
15	69 DANGUJE - 9 danguj	5410182107
16	СЕКТОР ГАЗА - 30 лет	5410182358
17	PAKITO - Living on Video	5410182305
18	Oggy	5410181062
19	Д.Билан - Ты должна рядом быть	5410181742
20	ДИМА БИЛАН - Я так люблю тебя	5410182384

ĮVAIRIOS MELODIJOS

NAUJIEJI LIETUVIAI - Apie norą	5410182394
DELFINAI - Jei liūdesys tave sušildo	5410182388
NAUJIEJI LIETUVIAI - Mergaitės	5410182386
NL - Neik šiandien į kastingus	5410182368
MOKINUKĖS - Ar mane matei	5410182352
TATU - Loves Me Not	5410182392
MAMA ROCK'N'ROLL - Mano gitara	5410182373
Ž. ŽVAGULIS - Alaus danguje nėra	5410181690
БЛЕСТЯЩИЕ - Восточные сказки	5410182176
FAKTOR - Krasavica	5410181605
BOB SINCLAR - Rock This Party	5410182376
FREDDIE MERCURY - Love Kills	5410182391
BODYROX - Yeah Yeah	5410182390
ROBBIE WILLIAMS - Rudebox	5410182377
PINK - U & Ur Hand	5410182371
JUSTIN TIMBERLAKE - Sexy Back	5410182370
IIO - Is It Love	5410182362
THE SIMPSONS - Theme	5410182360
TIESTO - He's A Pirate	5410182354
MARY J BLIGE FEAT U2 - One	5410182351
MARTIJN TEN VELDEN - I Wish You Could	5410182350
BRAINSTORM - Thunder Without Rain	5410182348
WESTBAM - United States Of Love	5410182342
BENASSI BROS FEAT SANDY - Feel Alive	5410182336

SMS TONAI

Lietutis	5410181431	Varpeliai	5410181420
Tik tak tik tak	5410181424	Linksma pabaiga	5410181419
Standartinis sms	5410181423	Pergalė	5410181418
Medinis skambesys	5410181422	Greitoji medicinos pagalba	5410181417
Pianino garsai	5410181421	Buksuojantis signalas	5410181416

MONOTONINĖ
1. **Rašyk žinutę su: M ir kodu:** Pvz.: M5410182374, draugui: M5410182374 370699XXXXX
2. **Siųsk numeriu: 1390**

POLIFONINĖ WAP/GPRS
1. **Rašyk žinutę su: P ir kodu:** Pvz.: P5410182374, draugui: P5410182374 370699XXXXX
2. **Siųsk numeriu: 1390**

2 Lt

MELODIJOS MONOTONINĖS: NOKIA: visiems modeliams
MELODIJOS POLIFONINĖS: NOKIA, SAMSUNG, MOTOROLA, SIEMENS, SONY-ERICSSON,LG, PANASONIC: su WAP nustatymais

JAVA ŽAIDIMAI

ASPHALT 3 Street Rules

LG: c1300. **Motorola:** c650, c650, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100,3120, 3200, 3220, 3230, 6020, 6030, 6060, 6100, 6230, 6230i, 6600, 6610, 6630, 6670, 6680, 7210, 7250, 7260, 7610, n70. **Samsung:** d500, d500e, d600, e330, e630, e700, e800, x460, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600.

J5410181223

Gangstar Crime City



Motorola: c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 6020, 6030, 6060, 6100, 6230, 6230i, 6600, 6610, 6630, 6670, 6680, 7210, 7250, 7260, 7610, n70. **Samsung:** d500, d500e, d600, e330, e630, e700, e800, x460, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600.

J5410181228

Sexy Vega$

Motorola: c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3510i, 6020, 6030, 6100, 6220, 6230, 6230i, 6610, 6630, 6680, 7210, 7250, 7260, n70.**Samsung:** d500, d600, e330, e630, e700, e800, x460, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** j300i, k300i, k500i, k600i, s700i, t610,t630, v800, w550i, w800, w800i, w810i, w900i, z600, z800.

J5410181209

Medžioklės sezonas atidarytas!



LG: c1300. **Motorola:** c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 5100, 6020, 6030, 6100, 6220, 6230, 6230i, 6600, 6610, 6610i, 6630, 6670, 6680, 6800, 6820, 7210, 7250, 7260, 7610, 8800, n70. **Samsung:** d500, d500e, d600, e330, e630, e700, e800, x460, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600, z800.

J5410181225

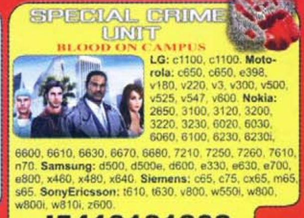
Rayman Raving Rabbids



LG: c1300. **Motorola:** e398, v3, v300, v500, v525, v547, v600.**Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 6030, 6060, 6100, 6230, 6230i, 6600, 6610, 7210, 7250, 7260. **Samsung:** d500, d500e, e330, e630, e700, e800, x460. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600, z800.

J5410181299

Special Crime Unit: Blood on Campus



LG: c1100, c1100. **Motorola:** c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 6020, 6030, 6060, 6100, 6230, 6230i, 6600, 6610, 6630, 6670, 6680, 7210, 7250, 7260, 7610, n70. **Samsung:** d500, d500e, d600, e330, e630, e700, e800, x460, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600.

J5410181302

Models-2



Motorola: e398, v3, v300, v500, v525, v547, v600, v620. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 5100, 6020, 6030, 6060, 6100, 6200, 6220, 6230, 6230i, 6600, 6610, 6610i, 6630, 6670, 6680, 6800, 6820, 7200, 7210, 7250, 7260, 7600, 7610, 8800, n70, n90. **Samsung:** d500, e330, e630, x480, x640. **Siemens:** c65, cx65, cx70, m65, s65. **Sony-Ericsson:** k300i, k500i, k700i, s700i, t610, t630, v800, w550i, w800, w800i, w810i, w900i, z1010, z600, z800.

J5410181282

Sexy Blocks: Cancun Vibes



LG: c1100, c1100. **Motorola:** c650, c650, e398, v180, v220, v3, v300, v500, v525, v547, v600. **Nokia:** 2650, 3100, 3120, 3200, 3220, 3230, 6020, 6030, 6060, 6100, 6230, 6230i, 6600,6610, 6630, 6670, 6680, 7210, 7250, 7260, 7610, n70. **Samsung:** d500, d500e, d600, e330, e630, e700, e800, x460, x480, x640. **Siemens:** c65, c75, cx65, m65, s65. **SonyEricsson:** t610, t630, v800, w550i, w800, w800i, w810i, z600.

J5410181303

1. **Rašyk žinutę su kodu:** Pvz.: J5410181225, draugui: J5410181225 370699XXXXX
2. **Jei priklausai OMNITEL ar BITĖ, siųsk numeriu: 1390**
Jei priklausai TELE2, siųsk numeriu: 1399

WAP 10 LT

WAP/GPRS

SOS ➡ support@ra7.lt

Įsitikinkite, kad telefone įjungta **WAP/GPRS** paslauga. Ją užsisakykite paskambinę savo operatoriui: **TELE2 - 117, OMNITEL - 1566, BITĖ GSM - 1501**. Paslauga tinka visiems OMNITEL, BITĖ LIETUVA, TELE2 klientams, išskyrus MAŽYLIO vartotojus.

PRAMONINIO ŠNIPINĖJIMO TECHNIKA

TARNYBINĖS INFORMACIJOS GAVIMO BŪDAI

PRAMONINIS ŠNIPINĖJIMAS EGZISTUOJA — TAI FAKTAS. IR JUO UŽSIIMINĖJA NE TIK (IR NE TIEK) Į DŽEIMSĄ BONDĄ PANAŠŪS GRAŽUOLIAI, BET IR PAPRASTI HAKERIAI, KURIE PRAKTIŠKAI NIEKADA NEIŠEINA IŠ NAMŲ IR VISUS SAVO VEIKSMUS ATLIEKA PER TINKLĄ. KARTAIS TAIP DAROMA IŠ SMALSUMO, KARTAIS — IŠ BŪTINYBĖS ARBA NORO UŽSIDIRBTI. TAPTI ŠNIPU GALI KIEKVIENAS, BEJE, VISIŠKAI TEISĖTU PAGRINDU!

Per pastaruosius dešimt metų pasaulis smarkiai pasikeitė, o kartu su juo pasikeitė ir pramoninio šnipinėjimo tikslai bei užduotys. Dabar jau niekas nedaro paslapties iš naujo produkto išleidimo laiko arba vartotojiškų charakteristikų, kaip kad tai būdavo ankstyvosios MS-DOS jaunystės laikais, kurios kūrėjams taip ir neleido pamatyti IBM PC prototipo.

Tarkim, šnipai sugebėjo gauti visą dokumentacijos komplektą arba bent jau patį pavyzdį, bet... ką su juo daryti? Be atitinkamos infrastruktūros ir „žinių nešiotojų" — savo galvose visas projekto detales saugančių inžinierių — tai tiesiog popierių krūvos ir metalo laužas, kurį norint išstudijuoti ir suvokti tektų sugaišti tiek pat laiko, kiek ir pasišovus iš naujo sukurti. Šnipinėjimas ir perėjimas prie vakarų technologijų kopijavimo galų gale lėmė buvusios SSRS skaičiavimo technikos pramonės žlugimą: juk net jeigu pavyktų nugvelbti patį naujausią pavyzdį, tai per „atvirkštinio projektavimo" (*reverse engineering*) laiką svetima inžinerinė mintis pajudėtų toli į priekį, o mes liktume nieko nepešę :). Be to, buvusioje Tarybų Sąjungoje viskas, kas buvo pavogta iš Vakarų, skaitėsi visų tautų nuosavybe, o į patentus niekas nekreipė dėmesio.

Apie patentus, korporacijas ir NDA

Dabar amerikiečių korporacijų įtaka visam pasauliui tokia, kad išleidinėti produkciją, bandant išvengti patentuotų technologijų licencijavimo, galima tik kokiame nors Kinijos rūsyje, ir tai tik iki tos akimirkos, kol teisių turėtojas nepateiks teismui ieškinio, kas visiškai sunaikina pramoninio šnipinėjimo prasmę, kadangi patentavimo



esmė — tai technologijos atskleidimas mainais į monopolišką nuosavybės turėjimo teisę. Tai reiškia, kad jeigu technologija neužpatentuota ir laikoma paslaptyje, bet kuris, kam pavyks ją gauti (pavyzdžiui, šnipinėjant arba naudojant „atvirkštinį projektavimą") gali netrukdomas ja naudotis. Ir priešingai, jeigu technologija yra užpatentuota, tuomet ji prieinama visiems pageidaujantiesiems ir su ja galima laisvai susipažinti (tam netgi nereiks nieko mokėti — patentų tekstai laisvai pateikiami internete). Tačiau... bet kokia praktinio pritaikymo forma (nesvarbu, ar komercinė, ar ne) reikalauja patento savininko licencijos, kuris turi teisę už ją paprašyti bet kokios pinigų sumos arba tiesiog atsisakyti tokią licenciją suteikti dėl „politinių" arba rinkodaros sumetimų.

Viskas, kas nėra patentuojama (pavyzdžiui, programų išeities tekstai), gali būti gauta remiantis NDA (*Non–Disclosure Agreement* — susitarimas dėl informacijos neatskleidimo), ko gavimas tiesiog stebina ir iš esmės yra grynai formali procedūra. Būtų labai klaidinga manyti, kad *Windows* išeities tekstai yra didelė „Microsoft" kruopščiai saugoma paslaptis. Jeigu „Microsoft" ką nors ir saugo, tai yra platinimas, ir visiškai ne atskleidimas. Gauti priėjimą prie išeities tekstų per NDA — visiškai realu. Pakanka prisiminti kompaniją „VMWare", per kurios skylėtą serverį įvyko informacijos nutekėjimas. Dėl taip susiklosčiusių aplinkybių *Windows 2000* kodas tapo prieinamas visiems pageidaujantiesiems. Kaip ten bebūtų, naudotis Džeimso Bondo pagalba tam visiškai nebūtina. Legalūs keliai greitesni, efektyvesni ir patikimesni, bet kokiu atveju, teoriškai reikalai yra būtent tokie. Tačiau ką gi mums pateikia realybė?..

Įsivaizduokime remonto dirbtuvių darbuotoją, ieškantį pagrindinės naujo „Sony" televizoriaus schemos, arba programuotoją, kuriantį ATI vaizdo plokštei skirtą *Linux* tvarkyklę. Ir nors tiek televizoriaus aptarnavimo dokumentacija, tiek techninė vaizdo plokštės specifikacija pačios savaime paslaptimi nėra laikomos, tokios informacijos gavimas per oficialius kanalus atsiremia į biurokratizmo sienas, kas labai dažnai atima kur kas daugiau laiko ir pastangų, nei *reverse engineering*. Logiškai mąstant, „Sony" suinteresuota parduoti kiek įmanoma daugiau televizorių, o tam reikia mokėti juos remontuoti, nes priešingu atveju jų atsisakys tiek pirkėjai, tiek ir pardavėjai. ATI suinteresuota parduoti kiek įmanoma daugiau vaizdo plokščių, ir nors ji atkakliai ignoruoja *Linux* egzistavimą, nenorėdama investuoti pinigų į tvarkyklių kūrimą, kvaila praleisti galimybę daugiau parduoti tiesiog trukdant kitiems kurti tvarkykles. Prie vairo stovintys žmonės tai puikiai supranta, tačiau specifikacijų dalinimu jie neužsiima, o pasiekti ko nors iš klerkų beviltiška. T.y. gauti specifikacijas per NDA įmanoma, tačiau kam jos mums reikalingos su NDA?

Pramoninio šnipinėjimo poreikis, kuris iš esmės sumažėjo „aukštame korporatyviniame lygyje", išliko aktualus pavieniams asmenims ir nedidelėms kompanijoms. Būtent apie tai mes ir pakalbėsim!

Ne tiek jau daug tų per tinklą realizuojamų pramoninio šnipinėjimo būdų, ir jie toli gražu ne tokie efektyvūs, kaip to paties Bondo tipo žvalgai, tačiau su aukščiau aprašytomis užduotimis šie būdai kuo puikiausiai susidoroja, nesukeldami jokių konfliktų su įstatymu, kas juos padaro dvigubai pavojingesnius!

Tvirtovės imamos iš vidaus

Korporatyvinė politika — tai tik matoma didelės mašinos dalis, kurią judėti priverčia paprasčiausi žmonės, bendraujantys vienas su kitu, aptariantys technines problemas arba tiesiog šnekantys apie įvairius dalykus, toli pasiųsdami slaptumą ir kitas kompanijos nuostatų diktuojamas taisykles. Daugelis užduočių išsprendžiamos bendromis kaimyninėse arba net konkuruojančiose kompanijose dirbančių inžinierių pastangomis. Praktika rodo, kad labai dažnai konkurencija kompanijos viduje kur kas didesnė, nei jos



Tipiško pramoniniu šnipinėjimu užsiiminėjančio hakerio darbo vieta

Hakeriai dirba tamsoje, apčiuopomis surasdami klavišus



Hakeriško urvo gilumoje

išorėje. Tipiška situacija: inžinieriui skyrė užduotį, su kuria jis nesugeba susidoroti. Tai pripažinti — reiškia pripažinti savo nekompetentingumą. Kreiptis pagalbos į kolegas — kur gi tau jie padės, o jeigu ir padės, tai tik dėl savo karjeros kilimo kitų sąskaita. Kaip sakoma, neturėk šimto pinigų, o geriau turėk šimtą draugų, net jeigu jie dirba kitame kontinente ir pažįstami tik per internetą. Juk vis tiek kiekvienas inžinierius vienaip ar kitaip ilgainiui prisirenka tinklinių pažinčių. Net jeigu jis ir neeikvoja savo laiko forumams, tai bent jau skaito techninę literatūrą — knygas ir straipsnius — o ten dažniausiai pateikiamas elektroninio pašto adresas.

Žinoma, pasitaiko pačių įvairiausių žmonių. Tarp jų yra ir dosnių, ir šykščių, ir tiesiog ožių, iš kurių neišspausi nė gramo naudingos informacijos. Tačiau surasti demokratiškai nusiteikusį žmogų, kuris mėgtų savo darbą ir kuris draugystę laikytų aukščiau kompanijos interesų, nėra sunku. Žinoma, naivu tikėtis, kad kas nors paprasčiausiai tiesiog šiaip sau padės perduoti pilną išeities tekstų (dokumentacijos, principinių schemų) komplektą, vien jau dėl to, kad egzistuoja tokia sąvoka, kaip priėjimo kontrolė, ir kiekvienas dirba tik su tomis projekto dalimis, kurioms jis „skirtas". Priešingu atveju galima sulaukti visiškos betvarkės, kai vienas nuskriaustas darbuotojas galės išdurti visą kompaniją.

Arabai tokiais atvejais sakoma: „Nori patekti pas karalių — susipažink su durininku". Neturinte durininko? Tiks ir sistemos administratorius. Papasakosiu realiai gyvenime nutikusį atvejį. Kartą man teko gauti vienos įrangos dokumentaciją, kuri buvo pateikiama tik su NDA ir tik kompanijoms partnerėms. Tapti partneriu neketinau, todėl teko apsiriboti susirašinėjimu su sistemos administratoriumi, kurio kontaktus gavau per kitus kompanijos darbuotojus, su kuriais susipažinau per svetainėje pateiktus viešus adresus. Administratorius (kaip ir priklauso) buvo nekalbus ir niūrus, kaip audrą žadantys debesys. Vis dėlto jo niūrumo priežastis buvo toli gražu ne meilės problemos, o reguliariai lūžtanti NT. Kaip žinia, paskutiniuose pataisymo paketuose buvo sugriežtinta klaidų kontrolė, todėl jau atlaisvintos atminties atlaisvinimas, kuris anksčiau tvarkyklėms nieko rimto nepridirbdavo, dabar sukeldavo BSOD. Ir tai buvo daroma mūsų bendram labui! „Microsoft" pamanė, kad jau geriau sustabdyti sistemą, negu leisti tvarkyklei išdykauti su atmintimi! Visa problema tame, kad ši tvarkyklė valdė sudėtingą aparatūrą, kurios techninio palaikymo laikotarpis jau seniai pasibaigė, todėl viskas, ką galėjo pasiūlyti šios įrangos tiekėjas — tai nusipirkti naują aparatūrą kartu su nauja tvarkyklės versija. Pastarosios kaina buvo gana nemaža, be to, ji buvo nesuderinama su kai kuria naudojama įranga.

Pataisymo paketo atsisakymas išspręsdavo BSOD problemą, tačiau palikdavo daugybę atvirų skylių, kurioms „individualių" pataisymų nebuvo, kitaip tariant, šie pataisymai turėjo priklausomybes, kurios sukeldavo branduolio OS pakeitimą ir atnaujintos versijos įdiegimą su sugriež-





NTKRNLOS.EXE taisymas su soft-ice

tinta kontrole. „Microsoft“ palaikymo tarnyba tik gūžčiojo pečiais — atseit, kam rūpi svetimos problemos, — ir visą atsakomybę perkeldavo ant tvarkyklių kūrėjų, kurių kaltė čia buvo akivaizdi ir neginčijama, tačiau tai nebuvo problemos sprendimas. Mėlynieji mirties ekranai toliau gadino gyvenimą, kompanija patirdavo nuostolius, administratorius gaudavo velnių ir... staiga scenoje pasirodžiau aš :).

Man, kaip hakeriui, sprendimas buvo akivaizdus. Reikėjo disasembliuoti branduolį, surasti tą vietą, kur atliekamas jau atlaisvintos atminties atlaisvinimas (o ją surasti labai paprasta — pagal kryžmines nuorodas į funkciją *KeBugCheckEx*, kuri iškviečiama su atitinkamu STOP kodu), ir šiek tiek pataisyti branduolį, prieš tai atjungtus įrašymo apsaugą nunulinant CR0 registro *WriteProtect* bitą. Aš nelaimingam administratoriui tiesiog pasiūliau man paštu išsiųsti jo NTKRNLOS.EXE, o po keliolikos minučių išsiunčiau „pataisytą“ variantą. Ne! Aš ten neįdėjau jokių slaptažodžius grobiančių užkratų, jokių *malware*. Vietoje to aš tiesiog paprašiau mane suvesti su tais žmonėmis, kurie galėtų padėti su dokumentacija. Štai ir viskas!

Manote, kad korupcija egzistuoja tik pas mus ir kad, pavyzdžiui, Azijoje nieko nevagia ir neima kyšių? Priešingai, ten tai daro visi, nė kiek nesigėdydami. Štai tik viena tos pačios kompanijos darbuotojo papasakota istorija: statant naują cechą projektuotojai meteorologų užklausė vidutinės metinės Tailando temperatūros. Remiantis gautais duomenimis buvo suprojektuota, pagaminta ir sumontuota kondicionavimo bei ventiliacijos sistema. Viskas būtų gerai, tačiau paaiškėjo, kad „vidutinė metų“ ir „vidutinė būdinga“ temperatūra labai skiriasi, kas ypač gerai jautėsi per vasaros karščius. Prasidėjo kaltų ieškojimas. Meteorologai nusiplovė iš karto — atseit, ko mūsų paklausėt, tą mes ir atsakėm, o projektuotojai rėmėsi tuo, kad nė velnio nesusigaudo meteorologiniuose terminuose ir tiesiog nežino, kaip „moksliškai“ vadinasi tai, ką jie turėjo galvoje. Viskas baigėsi tuo, kad projektuotojus atleido, o kondicionavimo sistemą demontavo, perprojektavo ir sumontavo iš naujo. Čia visa esmė tame, kad pirmoji sistema egzistavo tik ant popieriaus, o ar jūs bent nutuokiate fiktyvių gamybos/montavimo/demontavimo darbų kainą? Iš to daug kas pasipelnė! Tačiau mes šiek tiek nukrypome. Grįžkim prie mūsų šnipinėjimų.

Kiekvienoje firmoje galima rasti didelę techninę biblioteką, kurioje saugoma daugybė įvairių įdomių dalykų: tiek kuriamų produktų aprašymai, tiek ir išsami bibliografine retenybe tapusi dokumentacija. Nepaisant to, gauti šią informaciją labai paprasta — pakanka įkalbėti vieną kompanijos darbuotoją ten nueiti ir ką nors nukopijuoti. Paprastai šis prašymas yra patenkinamas, nors vadovybės požiūriu tai yra grubus pažeidimas, tačiau niekas apie tai jos nė nesiruošia informuoti. Dar vienas įmanomas variantas: galima susidraugauti su bet kokios stambios leidyklos darbuotojais ir taip nemokamai gauti elektronines naujausių knygų kopijas, kurias tavo bičiuliai tau išsiųs nemokamai, jeigu žinos, kad toliau tavęs jos niekur nenukeliaus.

Uždarą techninę dokumentaciją galima gauti per NDA, tačiau dėl šito kreiptis reikia ne per oficialius kanalus, o per kompanijos viduje dirbančius pažįstamus, kurie patars, į ką šiuo klausimu geriausia kreiptis. Kaip jau minėjau aukščiau, šiuolaikiniame technologijų pasaulyje informacija saugoma ne ją įslaptinant, o su patentais. Uždara dokumentacija lengvai pateikiama per NDA, jeigu, be abejo, veiksime ne per svetainėje pateiktų vadybininkų adresus — jie ir taip perkrauti



darbu. Papildomo vargo jiems visiškai nereikia. Kur kas paprasčiau prašymą tiesiog atmesti, nei įsitraukti į biurokratinį vilkinimą.

Dabar pakalbėkime apie neteisėtus būdus, bet ne tam, kad juos taikytume, o paprasčiausiai kad apie juos žinotume (kaip sakoma, atsarga gėdos nedaro). Be abejo, pirmoje vietoje yra nutolusios atakos. Šiuolaikinės sistemos skylėtos, administratoriai neišsilavinę ir/arba tinginiai, tai kodėl gi hakeriams nesuklestėjus? Ir vėl tas liūdnai pagarsėjęs žmogiškasis faktorius, leidžiantis be jokių įmantrybių įsiskverbti į korporatyvinį tinklą. Dažniausiai pakanka paprasčiausio į palaikymo tarnybą su prisegtu dokumentu išsiųsti laiško, ypač jeigu ten sėdi pagal skelbimą surinktos merginos. Visiškai nebūtina rašyti didelio boso vardu. Geriau apsimesti nieko nesuprantančiu briedžiu, kuris nori nusipirkti brangiai kainuojantį produktą, tačiau jam reiktų paaiškinti, kodėl jis reikalingas. Juk, vaizdžiai tariant, *Windows Server* ant lėkštutės nepadėsi. Ir problemų šis produktas sukelia tiek, kad nepadės net ir vazelinas. Oi! Apie ką aš čia? Ak, taip! Prieš įeidamas pagalvok, kaip išeiti (c) liaudies pasaka. Pakanka įsiklausyti į šią liaudies išmintį, juo labiau, kad panašią patarlę turi ir arabai: neatidaryk durų, kurių negalėsi uždaryti. Trumpiau! Prasiskverbti pro ugniasienę kur kas paprasčiau, nei išlįsti atgal. Jeigu tu nepateksi į medaus puodynę (kitaip tariant, į *honey-pot'ą*), tai prižadinsi Cerberį (t.y. įsilaužimų aptikimo sistemą — IDS), po ko teliks melstis vardan *proxy*, kad šis neišduotų tikrojo IP adreso, kadangi daugelis „anonimiškų" *proxy* jį išduoda. Be to, net ir likus nepastebėtam, toli gražu ne visada galima susiorientuoti korporatyviniame tinkle ir gauti ką nors konkretaus. Tačiau jeigu jau Alachas uždaro vienas duris, jis atidaro tūkstantį kitų, pasiųsdamas mums vedlį. O dar geriau — simpatišką, gerą vedlę. Tik štai kur šią gražuolę surasti? Jeigu nepadės vieši svetainėje pateikti adresai, tuomet reiktų pasirausti įvairiose pažinčių tarnybose, masiškai siuntinėjant laiškus-į-kuriuos-negalima-neatsakyti ir nustatant jų priklausomybę pagal antraštėse matomus IP adresus, kadangi daugelis poniučių rašinėja iš savo tarnybinio kompiuterio darbo metu. Beje, tai leidžia lengvai nustatyti jų geografinę buvimo vietą, ypač remiantis tuo faktu, kad visų pirma atėjus į darbą patikrinamas paštas, o tik tuomet daroma visa kita (nepamiršk apie laiko juostą: jie pateikia _labai_ daug informacijos).

Įsimylėjusi mergina gali daug. Reiktų būti tikru niekšu, kad pastūmėtum ją į tarnybinį nusikaltimą. Tačiau būna tokių žiaurių niekšų, kurie taip daro, o paskui ištirpsta pasauliniame voratinklyje kaip ryto rūkas.

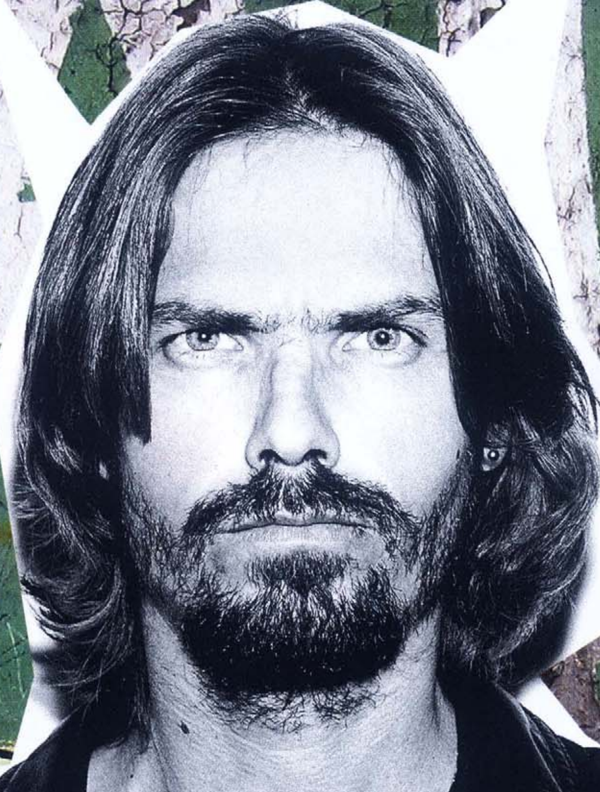
Kas pas mus toliau sąraše? Aha, šantažas. Tai purvinas ir visomis prasmėmis kriminalinis reikalas, tačiau atsiranda tokių ožių, kurie jo griebiasi, todėl tenka būti pasiruošusiam. Fiziniu susidorojimu grasinama retai, kadangi per internetą tai labai sunku įgyvendinti ir dar dėl to, kad su tokio pobūdžio grasintojais lengvai susidoroja policija.

Kur kas blogiau, jeigu šantažuotojas užsimins, kad jis pavydžiai žmonai gali pranešti apie išdavystę, prieš ką nepapūsi. Tuomet ir į policiją nenueisi. Yra daug skirtingų „sąžiningų" šantažo būdų. Pavyzdžiui, vaikui galima, kad jis galbūt įvaikintas. Pereinamuoju paauglio brendimo laikotarpiu, kai tėvų ir vaikų konfliktas ypatingai ryškus, toks į sielą įsiskverbęs abejonių kirminas gali sukelti labai rimtų pasekmių! Tačiau vis tiek geriau iš karto pasipriešinti šantažuotojui, negu kaip lėlei būti jo timpčiojamam už virvučių ir tikėtis, kad įvykdžius visus jo reikalavimus jis paliks jus ramybėje!

Pabaiga

Kiekvienam iš mūsų kartais tenka šiek tiek nusidėti ir veikti ne visai sąžiningais būdais. Jeigu gyvybiškai svarbiai programai sukurti reikalinga informacija, kurios nepavyksta gauti oficialiu keliu, telieka vadovautis tik bausmės griežtumu, padaugintu iš tikimybės būti sugautam, ir savo paties morale.

Įprastinė taktika, kurios laikosi praktiškai visos vakarų kompanijos, pavyzdžiui, ta pati „Cisco" ir „Microsoft": jeigu galima pirkti — perkam (savaime suprantama, už protingą kainą), jeigu ne — forsuojam Tiboro upę. Ir tegu kas nors pabando įrodyti, jog tuo metu mes nekasėm bulvių kaime pas močiutę. Beje, dėl *Cisco OS* išeities kodų vagystės kilęs skandalas susijęs su tuo, kad į šios OS sudėtį įeina nemažai iš *Linux* „pasiskolintų" komponentų, kurie (pagal licenciją) negali būti panaudoti uždaruose produktuose. Deja, teismai labai retai patenkina *Open Source* bendruomenės ieškinius, ir viskas dėl to, kad, vyriausybinės mašinos požiūriu, ji visai nereikalinga, kadangi, priešingai nei gigantiškosios kompanijos, ji nemoka mokesčių. Tačiau kas leidžiama Jupiteriui — negalima jaučiui. Taigi, geriau neliūdėkime, o leiskime gyvenimui tekėti sava vaga.



Kalėjimas velniukui



PANAUDOJAM „JAIL" TECHNOLOGIJĄ NESAUGIAI PROGRAMINEI ĮRANGAI PALEISTI

VAKAR SISTEMOS ADMINISTRATORIUS JONAITIS SULAIKĖ TRIS ĮTARIAMUOSIUS KONFIDENCIALIOS INFORMACIJOS ATSKLEIDIMU. SENDMAIL, WUFTPD IR PHP ŠIUO METU YRA IŠANKSTINIO SULAIKYMO KAMEROJE IR NEPRIPAŽĮSTA SAVO KALTĖS. PILIETIS JONAITIS UŽ PARODYTĄ BUDRUMĄ IŠ DARBDAVIO GAVO PREMIJĄ. NE, AŠ NESUPAINIOJAU ŽURNALO REDAKCIJOS ADRESO, PRADĖDAMAS STRAIPSNĮ TOKIA ĮŽANGA. ŠIANDIEN MES PAKALBĖSIM APIE, ATRODYTŲ, NESUDERINAMUS DALYKUS — APIE BSD SISTEMŲ ADMINISTRAVIMĄ IR KALĖJIMĄ (BE JOKIOS ABEJONĖS, APIE VIRTUALŲ, KAIP IR VISA KITA SKAITMENINIAME PASAULYJE). KALBĖSIME APIE JAIL TECHNOLOGIJĄ, NAUDOJAMĄ FREEBSD SISTEMOSE ATSKIRIEMS NESAUGIEMS SERVISAMS IZOLIUOTI NUO PAGRINDINĖS SISTEMOS.

Jail technologija turi daug pavadinimų. Tai ir tiesioginis vertimas — kalėjimas, ir šelmiškas — smėlio dėžė (*sandbox*), ir skambus — virtualus serveris. Šiaip ar taip, visi jie reiškia vieną — izoliuotą veikimo aplinką. *Jail* darbo principas pagrįstas sisteminio iškvietimo *chroot(2)* galimybe procesą ir jo palikuonis įkalinti į nuo pagrindinės sistemos atskirtą veikimo aplinką. Pavyzdžiui, nukopijavus visą sistemą į katalogą */usr/chroot* ir įvykdžius komandą „chroot /usr/chroot /bin/sh", mes atsidursime izoliuotoje aplinkoje, kurioje vykdomi veiksmai neatsilieps pagrindinei sistemai. Iš pirmo žvilgsnio tai puiki nesaugios programinės įrangos paleidimo platforma, tačiau *chroot* turi vieną esminį trūkumą — supervartotojo teisės čia neribotos. *Root* teises gavęs kenkėjas galės modifikuoti branduolį, užkrovinėti modulius, keisti tinklo konfigūraciją, montuoti failų sistemas ir net lengvai ištrūkti iš *chroot* aplinkos. O štai *jail* priešingai, iš supervartotojo atima daugybę privilegijų, taip lyg ir priskirdamas jį ypatingai vartotojų klasei. Kitaip tariant, būdamas *jail* aplinkoje *root* neturi teisės:

1./ Užkrovinėti branduolio modulių ir kaip nors modifikuoti branduolį (pavyzdžiui, per */dev/kmem*).

2./ Keisti branduolio kintamųjų (išskyrus *kern.securelevel* ir *kern.hostname*).

3./ Kurti įrenginių bylas.

4./ Montuoti ir demontuoti failų sistemas.

5./ Keisti tinklo konfigūraciją.

```
fbsd# jail /usr/jail/192.168.3.3 jail.jlm.org 192.168.3.3
# kldload sound
kldload: can't load sound: Operation not permitted
# sysctl kern.coredump=1
kern.coredump: 1
sysctl: kern.coredump: Operation not permitted
# mknod ad0 b 4 10
mknod: ad0: Operation not permitted
# mount -t ext2fs /dev/ad0s2 /mnt
ext2fs: /dev/ad0s2: Operation not permitted
# ifconfig ed0 inet alias 192.168.3.4 255.255.255.255
ifconfig: ioctl (SIOCAIFADDR): permission denied
# ping 192.168.3.1
ping: socket: Operation not permitted
# █
```

> Sargyba! Root prarado savo teises

6./ Kurti *raw* soketus (konfigūruojama galimybė).

7./ Prieiti prie tinklo resursų, kurie nesusieti su *jail IP* adresu.

8./ Dirbti su *System V IPC* (konfigūruojama galimybė).

9./ Prisikabinti prie proceso ir pasinaudoti *ptrace(2)*.

Kaip matome, *jail* aplinkoje *root* teisės labai ribotos, tačiau tokie pagrindiniai (ir daugeliu atvejų būtini) veiksmai, kaip priėjimo teisių ir limitų valdymas bei privilegijuotų tinklo jungčių panaudojimas *root* vartotojui yra prieinami. Griežtas administratoriaus teisių apribojimas *jail* viduje garantuoja, kad hakeris negalės ištrūkti iš apribotos aplinkos ir pakenkti pagrindinės mašinos veikimui. Be to, *jail* virtualizuoja mašinos tinklo resursus ir kiekvienai *jail* aplinkai reikalauja atskiro IP adreso. Būtent dėl šios priežasties *jail* dažnai vadina virtualiu serveriu.

Jail efektyviai išsprendžia su neprašytų svečių įsiskverbimu į pagrindinę mašiną susijusias problemas, tačiau jis niekaip neišgelbės nuo tų, kurie serverio resursus nori panaudoti savanaudiškais tikslais. Supervartotojas turi teises keisti limitus, todėl bet kuris *root* teises *jail* aplinkoje gavęs kenkėjas galės sistemą pakabinti su liūdnai pagarsėjusia *fork* bomba. *Jail* aplinkoje veikiantis SMTP serveris gali būti panaudotas spamui siuntinėti, o FTP serveris — paverstas į warezo saugyklą. Tai nėra didelė tragedija administratoriui, kuris stebi savo serverį, tačiau nereikšmingu dalyku to taip pat nepavadinsi. Šias problemas dalinai galima išspręsti iš kelių jail'ų sukuriant kažką panašaus į demilitarizuotą zoną (DMZ), tačiau tai jau visai atskiro straipsnio tema.

Asmeninis „jail“ serveris

Tikriausiai nedaugelis skaitytojų gali pasigirti turį iš karto keletą globaliai maršrutizuojamų IP adresų. Dėl šios priežasties jail'ui teks priskirti IP adresą iš A, B ir C klasės potinklių (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Paketai su tokiais gavėjo adresais niekada neatkeliaus iš išorinio pasaulio, kadangi dar kelio pradžioje juos sustabdys korektiškai sukonfigūruoti maršrutizatoriai. Taip pat mes turėsime transliuoti tinklo adresus (NAT) ir sukonfigūruoti per tam tikras (*destination*) jungtis įeinančių paketų nukreipimą į rezervuotą IP adresą iš privataus diapazono. Tegu šis adresas bus 192.168.3.3.

Norint sukurti naują *jail* aplinką, mums prireiks OS išeities tekstų. Iš jų mes sukompiliuosime pagrindinę *FreeBSD* aplinką ir įkelsime ją į specialiai tam skirtą katalogą, taip gaudami pagrindinės sistemos kopiją. Galima eiti ir kitu keliu: visus serviso paleidimui reikalingus dalykus nukopijuoti tiesiog iš pagrindinės sistemos, tačiau tai imlus darbui ir daug nesklandumų sukeliantis būdas, todėl mes jo kol kas atsisakysime. Taigi perkėlus iš disko arba parsisiuntus su *cvsup* išeities tekstus, pereikime į katalogą */usr/src* ir įvykdykime tokią komandų seką:

„JAIL“ APLINKOS SUFORMAVIMAS

```
# JAIL=/usr/jail/192.168.3.3
# mkdir -p $JAIL
# make world DESTDIR=
    $JAIL
# cd etc
# make distribution
    DESTDIR=$JAIL
# cd $JAIL
# ln -sf /dev/null kernel
```

Galiausiai kataloge */usr/jail/192.168.3.3* bus viskas, ko reikia naujam *jail* sukurti.






```
fbsd# mount -t procfs proc /usr/jail/192.168.3.3/proc
fbsd# jail /usr/jail/192.168.3.3 jail.j1m.org 192.168.3.3 /bin/sh /etc/rc
Loading configuration files.
Setting hostname: jail.j1m.org.
Starting syslogd.
ELF ldconfig path: /lib /usr/lib /usr/lib/compat
a.out ldconfig path: /usr/lib/aout /usr/lib/compat/aout
Starting local daemons:.
Updating motd.
Starting sshd.
Starting cron.
Local package initialization:.

Tue Jun 20 09:59:02 YEKST 2006
fbsd# ps ax | grep "J "
  630  ??  SsJ    0:00.08 /usr/sbin/syslogd -s
  682  ??  IsJ    0:00.01 /usr/sbin/sshd
  688  ??  SsJ    0:00.03 sendmail: accepting connections (sendmail)
  691  ??  IsJ    0:00.03 sendmail: Queue runner@00:30:00 for /var/spool/client
  698  ??  IsJ    0:00.04 /usr/sbin/cron -s
  709  v0  R+     0:00.03 grep J
fbsd# 
```

› Vaizdus jail serverio paleidimo pavyzdys

```
>> route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.3.0     *               255.255.255.0   U     0      0        0 tap0
localnet        *               255.255.255.0   U     0      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
>> nmap -P0 192.168.3.{2,3}

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2006-06-20 16:19 YEKST
Interesting ports on 192.168.3.2:
(The 1662 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
22/tcp open  ssh

All 1663 scanned ports on 192.168.3.3 are: filtered

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 44.277 seconds
>> 
```

› Nukreipimas sėkmingai veikia

Čia katalogo pavadinimas pasirinktas pagal IP adresą, kurį labai greitai mes priskirsime jail'ui. Šis pavadinimas gali būti bet koks, tačiau kuriant keletą jail'ų katalogo pavadinimo susiejimas su IP adresu arba servisu labai padeda administruojant.

Toliau tinklo sąsajai priskiriame IP pseudonimą (jail'o adresą). IP aljasai kuriami su komanda */sbin/ifconfig*:

```
# ifconfig ed0 inet alias 192.168.3.3 255.255.255.255
```

Kad nereikėtų vargintis ir šią komandą įvedinėti kiekvieną kartą po perkrovimo, pataisom */etc/rc.conf*:

```
# echo "ifconfig_ed0_alias0=\"inet 192.168.3.3\"" >> /etc/rc.conf
```

Taip pat reikia pašalinti konfliktus tarp pagrindinės mašinos ir *jail* aplinkos, pakeičiant kai kurių tinklo demonų konfigūraciją:

```
# echo „syslogd_flags=\"–ss\"" >> /etc/rc.conf
# echo „inetd_flags=\"–wW –a <x>\"" >> /etc/rc.conf
```

Pirmoji komanda *syslogd* demonui lieps neklausyti 514 jungties ir taip nepriimti logų iš kitų serverių (*syslogd* galima sukonfigūruoti ir taip, kad jis priiminėtų logus tik iš tam tikrų serverių). Antroji sukonfigūruoja *inetd* demoną, kad šis priimtų užklausas tik iš pagrindinės mašinos IP adreso. Bet koks pagrindinėje mašinoje veikiantis servisas taip pat turi būti atitinkamai sukonfigūruotas.

Kuriant jail'us taip pat būtina įvertinti jų specifiką, t.y. virtualią visos *jail* aplinkos esmę. Dėl to teks šiek tiek pasikapstyti katalogo */usr/jail/192.168.3.3/etc* viduriuose. Dabar pereiname į *jail* su supervartotojo teisėmis (įėjimas be inicializacinių skriptų paleidimo):

```
# jail /usr/jail/192.168.3.3 jail.j1m.org 192.168.3.3 /bin/sh
```

Komandai *jail* privalu pateikti keturis argumentus: kelią, domeno pavadinimą, IP adresą ir komandą, kuri bus įvykdyta įėjus į *jail* aplinką. Atsidūrus *jail* viduje, reikia įvykdyti keletą veiksmų:

1/ Sukurti tuščią *fstab* bylą (*touch /etc/fstab*), kad inicializacijos skriptai nesikeiktų, esą jos nėra.
2/ Sukurti supervartotojo slaptažodį (*passwd root*) ir, jeigu reikia, papildomus vartotojus.
3/ Perkonfigūruoti pašto aljasų bazę (*newaliases*), nes *sendmail* reikalauja, kad ji būtų.
4/ Sukonfigūruoti laiko zoną (*tzsetup*)..
5/ Taip paredaguoti */etc/resolv.conf*, kad *jail* viduje paleisti servisai galėtų išspręsti DNS vardus. Čia galima nurodyti pagrindinės sistemos IP adresą, jeigu joje veikia kešuojantis DNS serveris.
6/ Į */etc/rc.conf* pridėti šias eilutes:

```
# vi /etc/rc.conf

// jail tinklo vardas
hostname="jail.j1m.org"
// atjungiame tinklo sąsajų konfigūravimą (jie virtualūs)
network_interfaces=""
// paleidžiame reikiamus servisus
sshd_enable="YES"
```

Dabar galima išeiti iš *jail* aplinkos (komanda *exit*).

Nusikaltėlius kišam į jail'ą

Dabar viskas jau beveik paruošta serviso (šiuo atveju *ssh*) paleidimui *jail* aplinkoje. Teliko katalogo */usr/jail/192.168.3.3* viduje prie jau egzistuojančių montavimo taškų primontuoti virtualias failų sistemas, kad jų buvimo reikalaujančios programos veiktų be sutrikimų. Labiausiai reikli iš tokių VFS yra *procfs*, nors ir prie jos prieiti būtina tik nedaugeliui tinklo demonų. Jei būtina, prijunk *fdeskfs* ir *devfs*. Tiesa, su pastarąja reikia elgtis labai atsargiai, kadangi jos montavimas pagrindinės sistemos saugume gali sukurti rimtą skylę. Negalima kenkėjams leisti manipuliuoti įrenginių bylomis. Be to, kuriant jail'us visada reikia remtis taisykle „kuo paprasčiau, tuo patikimiau" ir atjungti viską, ką tik įmanoma.

Išsiaiškinę visus niuansus paleidžiam *ssh* serverį:

```
# mount -t procfs proc /usr/jail/192.168.3.3/proc
# jail /usr/jail/ftp jail.j1m.com 192.168.3.3 /bin/sh /etc/rc
```

Šį kartą mes nesiruošėme patys eiti į *jail* aplinką, todėl vietoje ketvirto argumento čia nurodytas ne „/bin/sh", o inicializacinius skriptus paleidžianti komanda. Dėl to ekrane turėtų pasirodyti diagnostiniai pranešimai, pranešantys apie tai, kad demonai (*sshd*, *syslogd* ir *cron*) buvo sėkmingai paleisti. Tuo taip pat galima įsitikinti žvilgtelėjus į komandos „ps ax | grep J" (visi *jail* viduje paleisti procesai gauna ‚J' vėliavėlę) išvedimą.

Dabar mes turime nuosavą neprieinamą *ssh* serverį, tačiau jis susietas su fiktyviu IP adresu. Norint klientams leisti jungtis prie šio serverio per viešą IP adresą, reikia sukonfigūruoti TCP tinklo srauto nukreipimą, ką lengva padaryti su iš *OpenBSD* atėjusiu *pf* ir kuris į *FreeBSD* buvo perkeltas ne taip seniai:

```
# vi /etc/pf.conf

ext_if="ed0"
host_ip="mūsų išorinis IP adresas"
```

```
jail_ip="192.168.3.3"
// ssh srautą nukreipiame į jail'o IP adresą
rdr pass on $ext_if inet proto tcp from any to
$host_ip \
 port ssh -> $jail_host
// Blokuojame visus likusius į išorinį tinklo inter-
feisą ateinančius prisijungimus
block in on $ext_if all
```

Jeigu dabar mes pabandytume iš nutolusios mašinos prisijungti į mūsų išorinio IP adreso *ssh* jungtį, tuomet paaiškėtų, kad viskas kuo puikiausiai veikia. SSH paketai nukreipiami, o kitos jungtys blokuojamos. Tai paprasčiausias ugniasienės konfigūravimo pavyzdys. Rimtesnėje konfigūracijoje taip pat tektų filtruoti ir iš grįžtamo ryšio kilpos (*loopback*) atkeliaujančius paketus (pagrindinė sistema su jail'u bendrauja būtent per loopback'ą).

Dabar beveik užbaigtą paveikslą papildykime dar vienu dalyku — sukonfigūruokime sistemą taip, kad ji *ssh* serverį paleidinėtų kiekvieno krovimosi metu:

```
# vi /etc/rc.conf
jail_enable="YES"
// jail aplinkų sąrašas
jail_list="ssh"
// standartinės jail opcijos
jail_ssh_rootdir="/usr/jail/192.168.3.3"
jail_ssh_hostname="jail.j1m.org"
jail_ssh_ip="192.168.3.3"
// kokias FS montuoti?
jail_ssh_devfs_enable="NO"
jail_ssh_fdescfs_enable="NO"
jail_ssh_procfs_enable="YES"
```

Mažos gudrybės

Ankstesniame skyrelyje mes jau aptarėme vartotojo galimybių apribojimo *jail* aplinkoje klausimą. Dabar visa tai aptarkime išsamiau. Pagal taisyklę „kuo paprasčiau, tuo patikimiau" galima sudaryti keletą taisyklių. Visų pirma, jei nebūtina, į *jail* katalogą nemontuok virtualių failų sistemų. Tikėtina, kad anksčiau ar vėliau vienoje iš jų bus surasta kritinė klaida, o tada tavo serveris gali būti sukompromituotas. Tas pats pasakytina ir apie *suid* programas — pasitaikius galimybei jas iš *jail* aplinkos derėtų pašalinti. Antra, paskirk šiek tiek savo brangaus laiko *jail* aplinkai išvalyti nuo visko, kas neturi įtakos serverio veikimui. Pirmu žingsniu link šio tikslo galėtų būti pagrindinės sistemos bylos */etc/make.conf* modifikacija su po to einančiu *jail* aplinkos perkompiliavimu. Taip, tai varginantis užsiėmimas, tačiau jis duoda savo rezultatus: taip apsunkinamas įsilaužėlių gyvenimas ir atlaisvinama vieta diske. Taip pat rekomenduojama visiems vartotojams sukonfigūruoti maksimalias naudojamų resursų ribas bei */etc* katalogo byloms suteikti maksimaliai griežtas priėjimo teises.

Mūsų pavyzdyje mes aptarėme *ssh* serverio įdiegimą į jail'ą, tačiau ką daryti tuomet, jeigu mums prireiks programos iš jungčių medžio? Kopijavimas — tai išlaidavimas, *symlink* sukūrimas neleistinas (*jail* aplinkos viduje jis rodys pats į save), NFS — tai situacijos apsunkinimas bei tuo pačiu dar vienos potencialios saugumo skylės sukūrimas. Yra paprastesnis būdas suteikti priėjimą prie jungčių medžio — *unionfs*:

```
# mount -t unionfs /usr/ports /usr/
jail/192.168.3.3/usr/ports
```

FreeBSD sistemoje yra keletas branduolio kintamųjų, kuriuos keičiant galima kontroliuoti branduolio elgseną *jail* aplinkos atžvilgiu. Ketvirtoje *fbsd* versijoje šie kintamieji turėjo priešdėlį *jail*. Pradedant penktąja versija, jų pavadinimo pradžia pasikeitė į *security.jail*. Žemiau pateikiamas šių kintamųjų sąrašas su aprašymais ir rekomendacijomis.

„Jail" kintamieji

security.jail.set_hostname_allowed — nurodo, ar supervartotojas gali keisti mašinos vardą (*hostname*). Nekenkia, jeigu *jail* aplinkai nėra išskirtas realus IP adresas, kuris būtų aprašytas DNS serverio zonose.

security.jail.socket_unixiproute_only — jeigu ši opcija įjungta, tuomet procesas turės teisę soketą kurti tik PF_LOCAL, PF_INET arba PF_ROUTE domenuose. Nėra prasmės išjungti šią opciją, kadangi praktiškai visos su tinklu veikiančios programos naudoja šiuos išvardintus domenus.

security.jail.allow_raw_sockets — jeigu opcija įjungta, tuomet supervartotojo procesas gaus teisę kurti *raw* soketus. Neveiks *ping*, tačiau tuo pačiu ir daugelis hakeriškų įrankių.

security.jail.sysvipc_allowed — aktyvavus, procesai gaus priėjimą prie *System V IPC*. Šią opciją įjungti ganėtinai pavojinga, kadangi *System V IPC* jail'e ir ne tik jame naudoja vieningą vardų erdvę, todėl teoriškai visi procesai (tiek veikiantys jail'e, tiek ir pagrindinėje sistemoje) galės bendrauti tarpusavyje.

security.jail.getfsstatroot_only — įjungus šią opciją procesai negalės gauti informacijos apie už *jail* ribų esančias failų sistemas. Tai apsaugos, pagrįstos informacijos nuslėpimu pavyzdys. *FreeBSD 6.0* versijoje ši opcija buvo pervadinta į *security.jail.enforce_statfs*.

security.jail.chflags_allowed — leidžia procesams modifikuoti FS vėliavėles (*chflags*). Atjungus šią opciją gauname galimybę *jail* kataloge kurti iš tiesų apsaugotas bylas. Kintamasis atsirado 5.4 ir 6.0 versijose.

security.jail.jailed — leidžia sužinoti, ar *sysctl* iškviečiantis procesas yra *jail* viduje.

INFO

Norint, kad pas tave veiktų pavyzdyje pateiktos paketų nukreipimo taisyklės, branduolį teks perkompiliuoti su ALTQ galimybe (options ALTQ).

Jail technologija pirmą kartą atsirado FreeBSD 4.0 versijoje.

Norint iš pagrindinės sistemos sustabdyti jail serverį, pakanka visus jail'o procesus nužudyti su komanda „kill -TERM".

FreeBSD 6.1 versijoje jail komanda pasipildė „-J" opcija, kuri leidžia į bylą išsaugoti jail aplinkos parametrus.

Kiekvienam servisui — kreiserinis greitis





KAIP OPTIMIZUOTI TINKLO SERVISŲ VEIKIMĄ

ŠIANDIEN MES PAKALBĖSIM APIE ĮVAIRIŲ TINKLO PROGRAMŲ DARBO OPTIMIZAVIMĄ. PRAKTIŠKAI KIEKVIENAS TINKLO SERVISAS TURI SAVAS NAŠUMO VALDYMUI SKIRTAS DIREKTYVAS. JŲ REIKŠMĖS PAGAL NUTYLĖJIMĄ APSKAIČIUOTOS VISIEMS: IR NAMŲ KOMPIUTERIUI, KURIAME VIENAS AR KITAS SERVISAS DAŽNIAUSIAI NAUDOJAMAS TIK EKSPERIMENTAMS, IR DIDELĖS ĮMONĖS SERVERIUI, PRIE KURIO VIENU METU PRIEINA ŠIMTAI VARTOTOJŲ. VISIŠKAI AKIVAIZDU, KAD TOKIE NUSTATYMAI NEGALI BŪTI OPTIMALŪS BŪTENT TAVO ATVEJUI. ŠIAME STRAIPSNYJE MES PAŠNEKĖSIM, KAIP IŠSPAUSTI MAKSIMALŲ NAŠUMĄ IŠ APACHE, PROFTPD, SAMBA IR OPENSSH.

Iš visų galimų FTP serverių realizacijų aš pasirinkau *ProFTPD*. Jeigu tu teiki pirmenybę *wu-ftpd*, *pure-ftpd* arba *vsftpd*, tuomet nesijaudink — jie konfigūruojami analogiškai. Atsidarome konfigūracijos bylą (mūsų atveju */etc/proftpd.conf*). Pirma, kas krenta į akis — tai direktyva *ServerType*. Jos reikšmė gali būti *standalone* arba *inetd*. Pagal nutylėjimą naudojama pirmoji, kuri reiškia, kad serveris veiks autonomiškai, o ne per *xinetd*. Jeigu dėl kokių nors priežasčių tavo konfige nurodyta *inetd*, tuomet tuojau pat ją pakeist į *standalone*. Autonominiam režime FTP serverio našumas žymiai didesnis, kadangi jis pastoviai užkrautas į atmintį ir laukia prisijungimų. Tuo tarpu *inetd* režime FTP serverį, priklausomai nuo poreikio, (kai gaunama užklausa) paleidžia superserveris *xinetd*. Akivaizdu, jog pastaruoju atveju užklausos apdorojimui sugaištama daugiau laiko.

Ar tau neatrodo, kad autorizacija serveryje trunka per daug laiko? Šį procesą galima iš esmės paspartinti atjungus direktyvas *IdentLookup* ir *UseReverseDNS*:

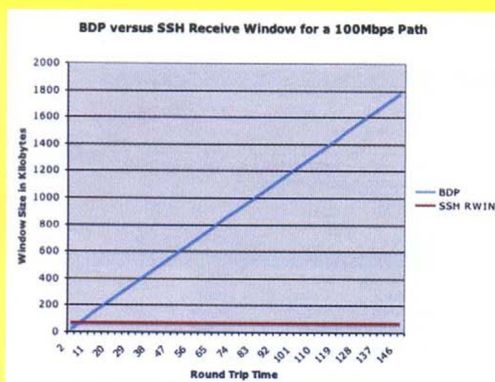
```
IdentLookups off
UseReverseDNS off
```

Pirmoji direktyva naudojama kartu su *ident* protokolu kliento identifikacijai. Kadangi šis protokolas vis tiek jau nenaudojamas, *IdentLookups* galima ramia sąžine išjungti.

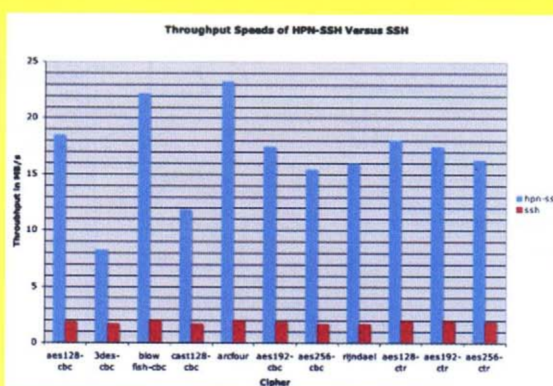
Antroji direktyva leidžia pagal prisijungusių klientų IP adresus nustatyti jų domeninius vardus. Kadangi vardų išsprendi-







> Skirtumas tarp mėlynos ir raudonos linijų byloja apie tuščiai išvaistytą pralaidumo potencialą



> SSH ir HPN–SSH našumas

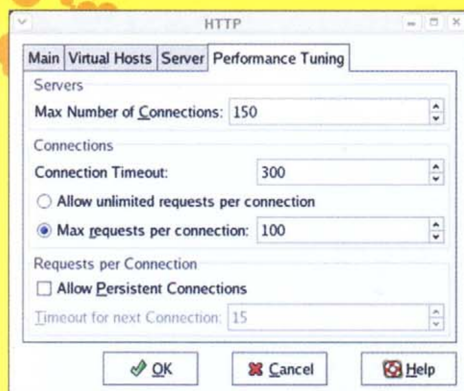
mas šiek tiek užtrunka, geriau jį atjungti — tuomet autorizacija serveryje vyks kur kas greičiau.

Vardų išsprendimą išsiaiškinom, judam toliau:

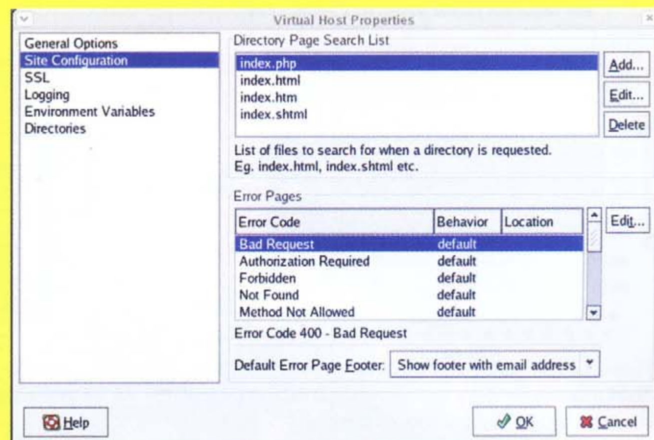
- **MaxClients skaičius [pranešimas]** — nurodo maksimalų vienu metu dirbančių klientų skaičių. Tai, kiek vienu metu dirbančių klientų gali išlaikyti tavo serveris, priklauso ne tik nuo paties serverio, bet ir nuo ryšio kanalo pralaidumo. Kuo „platesnis" kanalas, tuo su didesniu klientų skaičiumi gali susidoroti serveris.
- **MaxClientsPerHost skaičius [pranešimas]** — maksimalus iš vieno konkretaus tinklo mazgo besijungiančių klientų skaičius. Jeigu apribojimas bus viršytas, vartotojas pamatys pranešimą, kuris gali būti nurodomas, tačiau nėra privalomas. Ši reikšmė priklauso nuo kiekvieno konkretaus atvejo. Rekomenduoju iš vieno adreso leisti jungtis trims klientams.
- **MaxClientsPerUser skaičius [pranešimas]** — maksimalus prisijungimų skaičius iš vieno vartotojo. Gali čia nurodyti „1".
- **MaxConnectionRate skaičius** — leidžia nurodyti prisijungimų skaičių per sekundę. Šis parametras smarkiai priklauso nuo ryšio kanalo pralaidumo, todėl negaliu tau patarti, kokią konkrečią reikšmę geriau naudoti. Jeigu čia nurodytum „1", tuomet su serveriu per vieną sekundę bus galima užmegzti tik vieną susijungimą.
- **MaxHostsPerUser skaičius [pranešimas]** — maksimalus tinklo mazgų skaičius vienam vartotojui. Tarkim, išdykėlis Jonas Petraitis nori mus pergudrauti. Jis savo prisijungimo prie FTP serverio slaptažodį išdalino visiems savo pažįstamiems, todėl dabar jie bandys iš skirtingų kompiuterių prisijungti Jono vardu. Mes neleisime to padaryti, kadangi šį parametrą paliksime lygų „1".
- **MaxInstances skaičius** — maksimalus vienu metu paleidžiamų procesų skaičius *standalone* režimu. Siekiant išvengti *DoS* atakų, šio parametro parinkimui rekomenduoju skirti tinkamą dėmesį (ir vėl, jis priklauso nuo ryšio kanalo pralaidumo ir serverio pajėgumo). Mano konfige ši reikšmė lygi „30".
- **MaxLoginAttempts skaičius** — kiek kartų vartotojas gali mėginti įvedinėti slaptažodį. Po paskutinio bandymo serveris nutraukia susijungimą. Rekomenduojama reikšmė — „3".
- **MaxRetrieveFileSize** — maksimalus parsiunčiamos bylos dydis. Šio parametro galima nekontroliuoti, kadangi tavo į serverį perkeliamas bylas kontroliuosi tu pats, o vartotojų įkeliamų bylų dydį galima kontroliuoti su direktyva *MaxStoreFileSize*. Čia logika paprasta: jeigu niekas į serverį negalės įkelti, tarkim, 1 Gb dydžio bylos, tuomet atitinkamai niekas tokios bylos negalės ir parsisiųsti.
- **MaxStoreFileSize** — maksimalus bylos, kurią į serverį gali įkelti vartotojas, dydis. Čia viskas priklauso nuo kanalo pralaidumo ir laisvos vietos diske. Rinkis savo nuožiūra.

Jeigu serverio ryšio kanalas „siauras", tuomet situaciją galima kiek pagerinti su šiomis direktyvomis:

- **RateReadBPS baitai-per-sekundę** — apriboja maksimalų informacijos skaitymo greitį iš serverio (galiojimo sritis — serveris, *VirtualHost*, *Global*, *Anonymous*, *Directory*).
- **RateReadFreeBytes baitai** — nurodytas baitų kiekis nebus įvertinamas (apskaitomas; galiojimo sritis — serveris, *VirtualHost*, *Global*, *Anonymous*, *Directory*).
- **RateReadHardBPS off | on** — apibrėžia, ar po pirmųjų nemokamų baitų išeikvojimo laukti, kol vidutinis greitis nukris iki *RateReadBPS*, ar ne.
- **RateWriteBPS baitai-per-sekundę** — informacijos įrašymo į serverį greitis (galiojimo sritis — serveris, VirtualHost, Global, Anonymous, Directory).
- **RateWriteFreeBytes baitai** — tas pats, kas ir *RateReadFreeBytes*, tik įrašymui.
- **RateWriteHardBPS off | on** — tas pats, kas ir *RateReadHardBPS*, tik įrašymui.
- **TransferRate** — pakeičia senas *Rate** direktyvas ir leidžia apriboti maksimalų duomenų perdavimo greitį (skaitymui/rašymui). Kartais gali būti net ir nau-



› System–config–httpd: našumo konfigūravimas



› System–config–httpd: virtualaus serverio katalogo opcijos

dingiau pasinaudoti *Rate** direktyvomis, kadangi taip galima atskirai nurodyti skaitymo ir įrašymo greičius, kas naudinga, jeigu serveris prijungtas per asinchroninį kanalą.

Taip pat šiek tiek laiko galima išlošti, jeigu iš protokolo formato eilutės pašalintume „%h" modifikatorių (protokolo eilutė konfigūruojama su direktyva *LogFormat*). Tai kliento mazgo vardas, tačiau, kaip mes žinome, vardo išsprendimui reikalinga papildoma DNS užklausa, kam eikvojamas brangus laikas.

Teisingai sukonfigūravus aukščiau išvardintus parametrus, galima pasiekti esminio FTP serverio našumo prieaugio.

Steroidų prisivalgęs indėnas

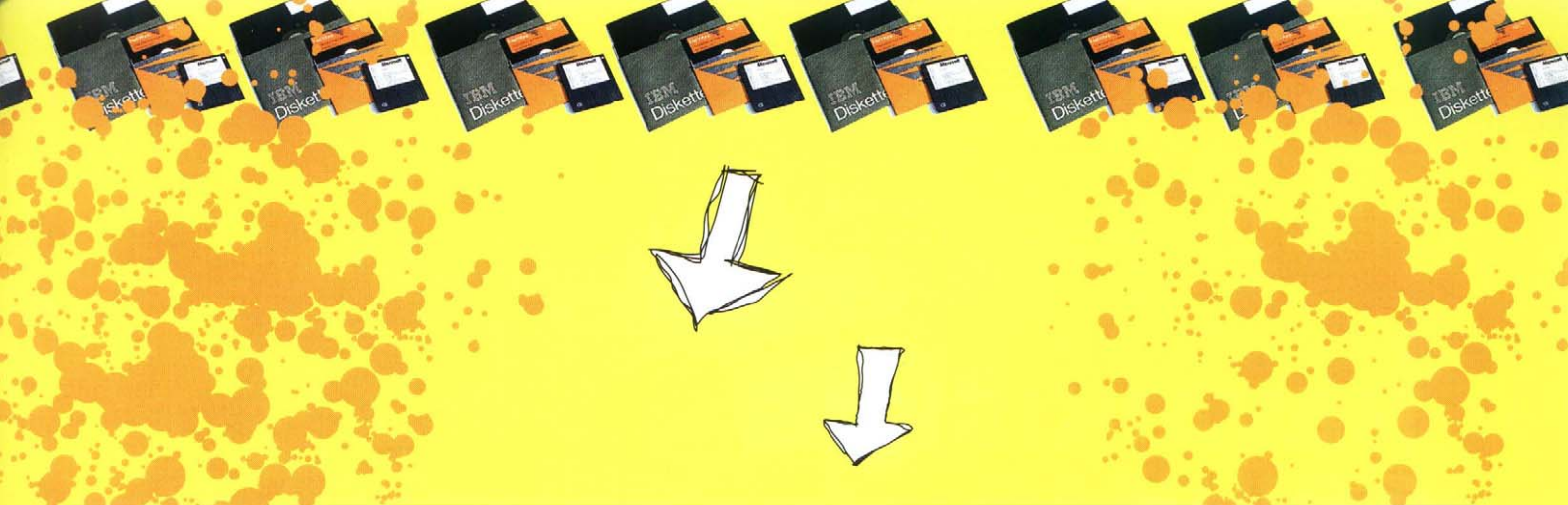
Kaip ir *ProFTPD*, *Apache* serveris turi *MaxClients* direktyvą, apibrėžiančią maksimalų vienu metu su serveriu galinčių dirbti klientų skaičių. Tačiau tai ne šiaip sau klientų skaičius, bet ir *Apache* procesų, vienu metu paleidžiamų tavo sistemoje, skaičius (t.y. kiekvienam prisijungimui skiriamas atskiras *Apache* procesas). Įsivaizduok, kad tu šią reikšmę nurodei lygią „30", o į tavo svetainę vienu metu bando prisijungti, tarkim, iš karto 35 vartotojai. Taip išeina, kad 5 vartotojai atsidurs „už borto". Kita vertus, jeigu tu šią reikšmę nurodysi su didele atsarga, tarkim, „150" arba net „200", o į tavo svetainę vienu metu užeina tik 5–10 vartotojų, tai bus neatleistinas sisteminių resursų švaistymas. Kam tau 190 dykinėjančių indėnų? Jie tik vartos brangius sisteminius resursus (procesoriaus laiką, operatyvinę atmintį). Dėl to reikia nustatyti maksimalų vartotojų skaičių, kuris kada nors buvo serveryje vienu metu. Tai galima padaryti su programa *Webalizer* arba su bet kokiu forumu, pavyzdžiui, PHPBB.

Žinoma, be *MaxClients* yra ir kitos našumo valdymo direktyvos. Pavyzdžiui, *StartServers*, *MaxSpareServers*, *MinSpareServers*. Kaip jau minėjau aukščiau, kiekvienam naujam susijungimui sukuriama nauja serverio proceso kopija. Direktyva *StartServers* nurodo tokį kopijų kiekį, kuris bus sukurtas paleidžiant pradinę serverio kopiją. Tuo pačiu pradinė serverio kopija gauna užklausas ir perduoda jas laisvoms kopijoms. Tai leidžia tolygiai paskirstyti apkrovimą atskiriems procesams bei padidinti visą serverio našumą. Tačiau praktikoje viskas nėra taip gerai, kaip norėtųsi — esminio našumo prieaugio galima tikėtis tik tuo atveju, kai serveris smarkiai apkrautas. Pagal nutylėjimą paleidžiamos penkios serverio kopijos.

Jeigu gaunamų užklausų skaičius viršija paleistų serverio kopijų skaičių, tuomet paleidžiami papildomi serverio procesai. Šie procesai nėra užbaigiami po savo užklausos apdorojimo, jie ir toliau lieka atmintyje. Direktyva *MaxSpareServers* leidžia nurodyti maksimalų tokių procesų skaičių. Jeigu šis skaičius viršytas, tada papildomi procesai yra užbaigiami. Jeigu serverių skaičius mažesnis, negu nurodyta su direktyva *MinSpareServers*, tuomet paleidžiamos papildomos kopijos. Norint, kad šios direktyvos veiktų, reikia, kad serveris būtų paleistas autonominiu režimu.

Direktyva *Timeout* nurodo laiko tarpą sekundėmis, per kurį serveris bando atkurti nutrauktą duomenų perdavimą. *Timeout* direktyva galioja ne tik duomenų perdavimui, bet ir priėmimui. Jeigu reikia perdavinėti dideles bylas, tuomet šią reikšmę reikia padidinti. Tačiau jeigu pas tave pats paprasčiausias *web* serveris, kuriame saugomi paskutinių distributyvų ISO atvaizdai, filmai ir kiti daug sveriantys dalykai, tuomet *Timeout* reikšmę galima sumažinti iki 30 sekundžių (pagal nutylėjimą šis parametras lygus 300 sekundžių).

Šiek tiek padidinti našumą gali padėti *KeepAlive* susijungimai (kitaip dar vadinami pastoviais susijungimais). Įprastinis susijungimas veikia taip: prisijungiam, išsiunčiam užklausą, atsijungiam. Tuo tarpu pastovaus susijungimo atveju per vieną susijungimą galima pasiųsti keletą užklausų ir gauti atsakymus. Kadangi šiuo atveju nėra kiekvieno proceso prisijungimo/atsijungimo procedūros, tai leidžia padidinti našumą. Pastovius susijungimus galima aktyvuoti su direk-



tyva *KeepAlive*, o su *KeepAliveTimeout* galima apriboti pastovaus susijungimo laiką (rekomenduojama reikšmė — 10–20 sekundžių).

Kad tavo indėnas pradėtų veikti dar greičiau, atjunk direktyvą *HostnameLookups*. *Apache* serveris logina kitų kompiuterių prisijungimus prie serverio. Aktyvavus šią opciją (*on*), į logą bus įrašomas kompiuterio–kliento domeno vardas. Jeigu ši opcija išjungta (*off*), tai į logą įrašomas kliento IP adresas. Šios opcijos aktyvavimas sulėtina serverio darbą, kadangi laikas sugaištamas laukiant atsakymo iš DNS serverio.

Dar greičiau šokam sambą

Pagrindinėje *Samba* konfigūracijos byloje (*smb.conf*) galima rasti parametrą „widelinks". Jeigu jį padarytume lygų „no", tuomet serviso našumas nukristų maždaug 30%, kadangi *Samba* nesektų simbolinių nuorodų neeksportuojamoje srityje. Norėdama nustatyti, kur yra nuoroda (ar prieinamoje srityje, ar ne), *Samba* iš pradžių seka šia simboline nuoroda, o po to įvykdo taip vadinamą „directory path lookup", kad nustatytų, kur ši nuoroda baigiasi. Ši operacija kiekvienam bylos lookup'ui reikalauja 6 papildomų sisteminių iškvietimų, o tokių užklausų *Samba* įvykdo labai daug.

Daugeliu atvejų *Samba* našumas priklauso nuo to, ar teisingai sukonfigūruoti TCP/IP protokolų steko parametrai. Jeigu užklausų ir atsakymų į jas dydis nėra fiksuotas, tuomet rekomenduojama pasinaudoti opcija TCP_NODELAY:

```
socket options = TCP_NODELAY
```

Testai rodo, kad *Samba* esant dideliems apkrovimams su šia opcija veikia 3 kartus greičiau. Jeigu *Samba* naudojama lokaliame tinkle (daugeliu atvejų būtent taip ir yra), tuomet taip pat rekomenduojama nurodyti opciją IPTOS_LOWDELAY:

```
socket options = IPTOS_LOWDELAY TCP_
NODELAY
```

Nori iš *Samba* išspausti dar daugiau? Tuomet nurodyk tokius buferizavimo parametrus: SO_RCVBUF su reikšme 8192 ir SO_SNDBUF su reikšme 8192, kaip parodyta žemiau:

```
socket options = TCP_NODELAY SO_RCV-
BUF=8192
 SO_SNDBUF=8192
```

Dešimteriopas SSH pagreitinimas

Iš *www.psc.edu/networking/projects/hpn-ssh/* svetainės galima parsisiųsti pataisymus (HPN-SSH projektas), kurie kopijavimą su SCP paspartina 10 kartų! Žinoma, šie patch'ai pritaikomi *OpenSSH* (*www.openssh.com/portable.html*) išeities tekstams. Tiesa, prieš įdiegiant HPN-SSH reikia šiek tiek „patiuninti" TCP/IP steką. Apie tai išsamiai pasakojama *www.psc.edu/networking/projects/tcptune/* puslapyje.

Toks našumo padidėjimas pasiekiamas pakeičiant SSH buferius arba atjungiant šifravimą bylų perdavimo metu. Taip pat yra pataisymas, kuris leidžia visiškai atjungti šifravimą bylos perdavimo metu (visi mes suprantame, kad saugumo požiūriu tai visiškai netikslinga).

Priversti SCP dirbti greičiau labai paprasta: parsisiunčiam ir išpakuojam pataisymo išeities tekstus, tada pritaikome pataisymą (žr. *man patch*). Po to reikia perkompiliuoti *OpenSSH*. Savaime suprantama, jeigu *OpenSSH* įdiegtas kaip paketas (iš RPM arba analogiško archyvo), tuomet prieš atliekant visus šiuos veiksmus reikia pašalinti atitinkamą RPM paketą. Beje, pritaikyti šiuos pataisymus ir perkompiliuoti *OpenSSH* reikia tiek serveryje, tiek ir kliente, nes priešingu atveju visas šis spartinimas neturi prasmės.

HPN–SSH projekto puslapyje galima rasti keletą pataisymų. Daugeliui vartotojų tiks HPN–11 pataisymas, kuris yra savotiškas kompromisas tarp našumo ir saugumo. Siunčiantis pataisymą būtinai atkreipk dėmesį į jo versiją — ji priklauso nuo tavo *OpenSSH* paketo. Norint aktyvuoti HPN–11 po *OpenSSH* perkompiliavimo, komandinėje eilutėje nurodyk ‚–R' parametrą *scp* atveju arba ‚–r' parametrą *ssh* atveju.

Pataisymas „HPN–11 with None Cipher" bylų perdavimo metu iš viso atjungia šifravimą. Čia šifruojamas tik per tinklą perduodamas vartotojo vardas ir slaptažodis. Po sėkmingos autentifikacijos šifravimas nėra naudojamas, todėl bylos per tinklą perduodamos atviru pavidalu. Tai pakankamai pavojinga, tačiau jeigu perduodama daug ir nekonfidencialios informacijos (pavyzdžiui, muzika arba vaizdas), tuomet šis pataisymas pasiteisina. Pritaikius šį pataisymą atjungti šifravimą galima su komandinės eilutės opcija ‚–z' (tiek *ssh*, tiek ir *scp* atveju).



NEVAIKIŠKAS TRIUKAS

APSUPTAS KOMPIUTERIŲ, APIPAINIOTAS LAIDŲ, AŠ SĖDĖJAU SAVO HAKERIŠKO URVO GILUMOJE IR REZGIAU ŽVĖRIŠKĄ PLANĄ, KURIS GALIAUSIAI LEISTŲ APLENKTI „MICROSOFT“! DAR IR KAIP APLENKTŲ! IMPORTO GREITIS SMARKIAI IŠAUGO, PUIKIAI DIRBDAMAS TIEK SENOVINĖJE 9X, TIEK IR „WINDOWS SERVER 2003“ SISTEMOJE, ĮSKAITANT VISAS TARPINES SISTEMAS, BEJE, NENAUDOJANT NĖ GRAMO ASEMBLERINIO KODO! VISAS 100% SU C!



SUPERGREITAS API FUNKCIJŲ IMPORTAS

„Microsoft“ klasta ir meilė

Aptarkime standartinės importo lentelės veikimą. Hierarchijos viršūnėje yra *Import Directory Table* struktūra, kuri yra IMAGE_IMPORT_DESCRIPTOR struktūrų masyvas, pasibaigiantis nuliniu elementu. Kiekviename IMAGE_IMPORT_DESCRIPTOR yra nuorodos į dvi pavaldžias struktūras — *lookup* lentelę (*Import Name Table*; čia saugomi importuojamų funkcijų vardai ir/arba ordinalai) ir importuojamų adresų lentelę (*Import Address Table*), kuri taip pat žinoma kaip *Thunk Table*. Užkraunant bylą čia įrašomi efektyvūs importuojamų funkcijų adresai.

Abi lentelės — tai 32 bitų dydžio elementų masyvai, kurių indeksai abipusiai vienas kitą atitinka, t.y. jeigu mums reikalinga funkcija *some_func* yra *lookup* lentelės i–tajame elemente, tuomet (užkrovus bylą į atmintį) importuojamų adresų lentelės i–indekse bus saugomas efektyvus virtualus *some_func* adresas.

```
typedef struct _IMAGE_IMPORT_DESCRIPTOR {
    union {
        DWORD Characteristics;
        DWORD OriginalFirstThunk;
    };
    DWORD TimeDateStamp;
    DWORD ForwarderChain;
    DWORD Name;
    DWORD FirstThunk;
} IMAGE_IMPORT_DESCRIPTOR;
```

Iki bylos užkrovimo į atmintį importuojamų adresų lentelė dubliuoja *lookup* lentelę, kas (teoriškai) leidžia užkrovikliui apsieiti tik su viena virtualių adresų lentele, taip išvengiant šuolių atmintyje, tačiau praktiškai jis ją ignoruoja.

Sukurkime paprasčiausią programą *test.c* ir sukompiliuokime ją su *Microsoft Visual C++* kompiliatoriumi su nustatymais pagal nutylėjimą:

```
#include <stdio.h>
main() { printf("hello, world!\n"); }
```

Sukurtą bylą *test.exe* praleisim per įrankį *dumpbin*, įeinantį į MS VC sudėtį (*dumpbin /IMPORTS test.exe > out*) ir pažiūrėsim, ką gero jis mums pasakys:

```
KERNEL32.dll
        405000 Import Address Table
        4054AC Import Name Table
        0 time date stamp
        0 Index of first forwarder reference
        2DF   WriteFile
        174   GetVersion
        7D    ExitProcess
```

Aha, adresų lentelė įsikūrusi adresu *405000h*, o *lookup* lentelė — *4054ACh* adresu. Žvilgtelėjus tenai su *hiew*, mes pamatome importuojamų funkcijų vardų RVA adresus. Abi lentelės visiškai sutampa ir rodo į importuojamų funkcijų vardų/ordinalų masyvą. O dabar su *dumpbin* apdorokime standartiškai su NT pateikiamą programą „Notepad“ (*dumpbin / IMPORTS notepad.exe > out*), po ko pamatysime, kokie skirtumai.

```
KERNEL32.dll
        1001080 Import Address Table
        1006784 Import Name Table
        FFFFFFFF time date stamp
        FFFFFFFF Index of first forwarder reference
77E99F42        1EF LocalUnlock
77E8B7F4        1AE GlobalUnlock
77E8CCA3        1A7 GlobalLock
```

Dar prieš bylos užkrovimą į atmintį adresų lentelėje jau saugojami paruošti efektyvūs virtualūs adresai! Jeigu netiki — pažiūrėk su *hiew'u*. Adresų lentelės turinys — efektyvūs virtualūs importuojamų funkcijų adresai! Dėl šios gudrybės sisteminiam užkrovėjui jau nebereikia eikvoti laiko funkcijų importui. Jis paprasčiausiai žiūri



į importuojamos DLL bibliotekos laiko žymės lauką (*TimeDateStamp*) ir, jeigu jis sutampa su kompiuteryje įdiegtos DLL laiku, realus importas nėra atliekamas. Žinoma, priešingu atveju tenka pasiraitoti rankoves ir užkrovimui eikvoti procesoriaus taktus, tačiau „Microsoft" savo taikomąsias programas atnaujina kartu su sisteminėmis bibliotekomis, todėl šios kompanijos programos turi didelį privalumą prieš konkurentus. Kokia klasta!

Tokia funkcijų importo technika vadinasi bindingu (*binding*), kuri prireikus gali būti įdiegta su įrankiu *editbin*, pasiskolintu iš to paties MS kompiliatoriaus (*editbin /BIND test.exe*). Pažiūrėkime, ką jis padarė su mūsų testine byla:

```
KERNEL32.dll
        405000 Import Address Table
        4054AC Import Name Table
        44B17B02 time date stamp
        13 Index of first forwarder reference
79446390C       2DF WriteFile
79450D1D        174 GetVersion
794569BE         7D ExitProcess
```

Po bindingo API funkcijų vardų RVA adresai pasikeitė į efektyvius virtualius pačių API funkcijų adresus. Nejaugi dabar mūsų programa krausis ne blogiau, nei pačios „Microsoft" programos? Ogi ne. Tai tavo sistemoje ji krausis „ne blogiau", o daugelyje likusių kompiuterių esančios DLL laiko žymė greičiausiai nesutaps su tavo bibliotekos laiko žyme, todėl visa optimizacija nueina šuniui ant uodegos, juo labiau, kad „Microsoft" turi tendenciją DLL atnaujinti ne tik su kiekviena operacinės sistemos versija, bet ir su eilinio pataisymų paketo įdiegimu! Atrodo, kad ši situacija — be išeities, tačiau taip nėra...

Kaip nušluostyti nosį „Microsoft'ui"

Pats paprasčiausias sprendimas — tai vilktis paskui save *editbin* (laimė, licencija to nedraudžia) ir atlikti bindingą prieš pat programos įdiegimą. Nenorintys prasidėti su „Microsoft" gali savarankiškai realizuoti bindingui skirtą įrankį arba pasinaudoti Jurijaus Charono sukurtu linkeriu ulink. Vis tik prieš atsidarant alų ir švenčiant pergalę susimąstyk: kas nutiks, jeigu vartotojas sistemą atnaujins po mūsų programos įdiegimo? Teisingai! Bindingai tuojau pat nustos veikti, krovimosi greitis smarkiai nukris, o tai nėra gerai. Žinoma, vartotojui galima parekomenduoti mūsų programą įdiegti iš naujo po kiekvieno operacinės sistemos atnaujinimo, tačiau tai nehumaniška ir apskritai žiauru. Kur kas paprasčiau pasielgti kiek kitaip. Tegu kiekvieno paleidimo metu mūsų programa tikrina visų importuojamų DLL bibliotekų *TimeDateStamp* lauką ir, jeigu jis pasikeitė, bindingų atnaujinimui paleidžia *editbin* (arba bet kokį kitą tai darantį įrankį). Kadangi aktyvaus proceso taisyti negalima, jį būtina užbaigti, prieš tai sukūrus dukterinį sub–procesą arba paleidus *bat* bylą, kuri re–bindintų mūsų programą ir tuojau pat ją vėl iš naujo paleistų, kad visi šie veiksmai vartotojo atžvilgiu būtų atliekami skaidriai ir nestumtų jo į išdavystę.

Ekstremalus optimizavimas

Disasembliavus *notepad.exe* arba mūsų optimizuotą *test.exe*, mes pamatysim, kad visos API funkcijos iškviečiamos netiesiogiai, kas visiškai nepadidina našumo.

```
.text:0040115F          push 0FFh
.text:00401164          call ds:[ExitProcess]
```

Tiesioginis funkcijos iškvietimas *call addr* yra kur kas greitesnis, negu *call [addr]* (ypač cikluose), tai kodėl gi nepaėmus ir neįskiepijus programai efektyvių API funkcijų adresų, kurie nustatomi įdiegimo stadijoje per *GetProcAddress*? Savaime suprantama, nereikia pamiršti laiko žymės kontrolės. Nė vienas man žinomas įrankis to daryti nemoka, todėl tenka judinti smegenis, miklinti pirštelius ir savarankiškai programuoti su *C*.

Analizuojant sukompiliuotos programos importo lentelę, surandame visas kryžmines nuorodas į API funkcijas ir, jeigu ten bus FFh 15h XXh XXh XXh XXh (netiesioginis *call*), vietoje jo įrašome EB YYh YYh YYh YYh 90h (tiesioginis CALL + NOP; kodėl mums reikalingas NOP? Ogi todėl, kad tiesioginis iškvietimas vienu baitu trumpesnis), kur YYh YYh YYh YYh — santykinis API funkcijos adresas, skaičiuojamas nuo instrukcijos CALL pabaigos. Po to atmetame importo lentelę, palikdami tik KERNEL32.DLL su vienintele importuojama funkcija (nesvarbu kokia). Esmė tame, kad sisteminis *Windows 2000* užkroviklis turėjo klaidą ir atsisakydavo užkrauti programas, kurios iš KERNEL32.DLL neimportuoja nė vienos funkcijos, o tai reiškia, kad ši biblioteka nėra projektuojama į savą adresų erdvę. Kadangi KERNEL32.DLL reikėjo pačiam užkroviklui, tačiau jis pamiršdavo tai patikrinti, ar ji apskritai buvo projektuojama į adresų erdvę, ar ne, tai programos be importo lentelės lūždavo su išimtimi (*exception*).

Finale mes: a) importo lentelės sąskaita sumažinsime bylos dydį; b) pagreitinsime bylos užkrovimą; c) šiek tiek optimizuosim API funkcijų iškvietimą (beje, kadangi triuškinančios API funkcijų daugumos vykdymas užima pagrindinę laiko dalį, skirtumas tarp tiesioginio ir netiesioginio iškvietimo nebus jau toks ir pastebimas, tačiau yra tokių API funkcijų, kurios susideda iš vos keleto eilučių, pavyzdžiui, *GetLastError*).

Pabaiga

Tau tik atrodo, kad *Windows* sistema išnaršyta skersai ir išilgai! Iš tikrųjų optimizavimo potencialas dar neišsemtas, todėl kūrybingai mąstantis programuotojas visada suras neįprastą sprendimą, savo greičiu aplenkiantį net ir pačią „Microsoft"!

Gelžbetoniniai objektai

LABAI DAŽNAI PROGRAMIŠKAI KURDAMI OBJEKTUS MES NESUSIMĄSTOME APIE SAUGUMĄ, PALIKDAMI JŲ PARAMETRUS OS NUOŽIŪRAI. TAČIAU PRIĖJIMO TEISIŲ VALDYMAS — NE TOKS JAU SUDĖTINGAS DALYKAS, REIKALAUJANTIS VISO LABO KELETO PAPILDOMŲ KODO EILUČIŲ IR ATITINKAMŲ FUNKCIJŲ ŽINOJIMO. PRIĖJIMO VALDYMO FUNKCIJŲ ŽINOJIMAS GALI PRAVERSTI NE TIK KURIANT OBJEKTUS, TODĖL ŠIANDIEN AŠ TAU PAPASAKOSIU APIE SID, SECURITY ATTRIBUTES, SECURITY DESCRIPTORS IR APIE VISKĄ, KAS SUSIJĘ SU ŠIOMIS SĄVOKOMIS.

SAUGUMO DESKRIPTORIAI IR IDENTIFIKATORIAI

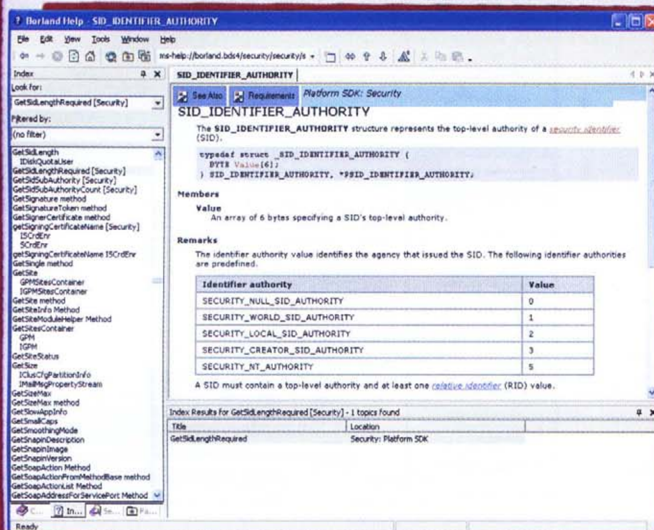
Saugumo atributai

Temos aptarimą pradėsime nuo pačios pabaigos, t.y. nuo bylos arba katalogo sukūrimo funkcijos. Abi funkcijos turi vienodą parametrą — rodyklę į SECURITY_ATTRIBUTES struktūrą. Funkcijoje CreateFile ši rodyklė iš eilės yra ketvirta, o funkcijoje CreateDirectory — antra. Kaip aš jau sakiau, daugeliu atvejų šis laukas paprasčiausiai ignoruojamas, tuo tarpu mes pažiūrėkim, kaip būtų galima jį tvarkingai užpildyti.

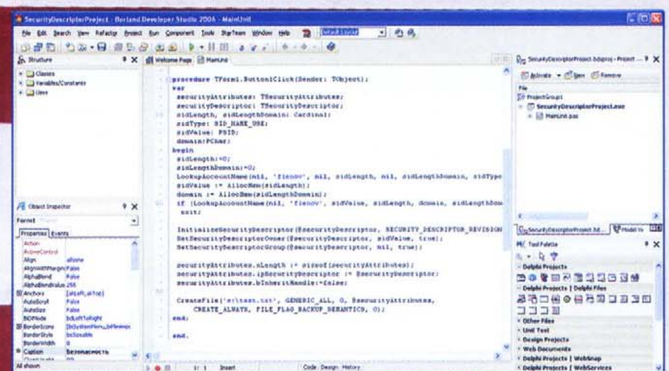
Kas tai per struktūra? Ji apibrėžia saugumo atributus ir susideda iš viso labo trijų laukų:

```
PSecurityAttributes = ^TSecurityAttributes;
_SECURITY_ATTRIBUTES = record
nLength: DWORD;
lpSecurityDescriptor: Pointer;
bInheritHandle: BOOL;
end;
```

Pirmasis laukas apibrėžia struktūros dydį. Panašius laukus galima sutikti daugelyje WinAPI struktūrų. Antrasis laukas — tai rodyklė į saugumo deskriptorių (security descriptor). Trečiasis parametras — loginė reikšmė, kuri nurodo, ar dukteriniai procesai gali paveldėti nurodytą saugumo deskriptorių. Pastarųjų paveldimumas mūsų šiandien nedomina ir išeina už šio straipsnio rėmų, todėl mūsų aptariamame pavyzdyje šio parametro reikšmė bus false.



> Informacija apie SID. Čia taip pat galima rasti iš anksto apibrėžtų identifikatorių sąrašą



> SID gavimo ir panaudojimo funkcijos kodas

Mums įdomiausias antrasis parametras, į kurį derėtų atkreipti ypatingą dėmesį. Tai rodyklė į saugumo deskriptorių, kurioje iš tiesų nėra nieko baisaus.

Saugumo deskriptorius

Kiekvienam OS objektui sukuriamas saugumo deskriptorius, pagal kurį nustatomos priėjimo prie objekto teisės, jo savininkas, grupė bei SACL (System Access Control List) ir DACL (Discretionary Access Control List) sąrašai. Mes aptarime programavimo pusę, todėl akcentuosime pačias funkcijas. Jeigu tave domina Windows sistemos saugumo teorija, tuomet tau reiktų pasiskaityti kokią nors adminams skirtą knygą arba apsilankyti

Taigi, pažiūrėkim, kas gi tas deskrip... programavimo požiūriu. Iš tiesų ta... struktūra, atrodanti štai taip:

```
PSecurityDescriptor = ^TSecurityDesc...
_SECURITY_DESCRIPTOR = record
  Revision: B...
  Sbz1: Byte;
  Control: SECURITY_DESCRIPTOR_CON...
TROL;
  Owner: PSID;
  Group: PSID;
  Sacl: PACL;
  Dacl: PACL;
end;
```

...byloje ...tūra apr... ...strakčiai. Iš ...sideda, ...tatyti tik pa... ...traščių ...pas.

...ime peržiū... ...reiškia v... ...u supras... deskrip... ...ą.

Revision — revizija. Šis parametras ... būti lygus vienetui, o dar geriau na... tis konstanta SECURITY_DESCRI...

OBJEKTŲ SUKŪRIMAS AKIVAIZDŽIAI NURODANT SAVININKĄ IR GRUPĘ

```
procedure TForm1.Button1Click(Sender: TObject);
var
  securityAttributes: TSecurityAttributes;
  securityDescriptor: TSecurityDescriptor;
  sidLength, sidLengthDomain: Cardinal;
  sidType: SID_NAME_USE;
  sidValue: PSID;
  domain:PChar;
begin
  // nunuliname buferių ilgį, kad nustatytumėm
  tikrą jų dydį
  sidLength := 0;
  sidLengthDomain := 0;

  // Pirmasis iškvietimas užbaigiamas su klaida,
  tačiau jis grąžina duomenų dydį
  LookupAccountName(nil, 'jonoUseris', nil,
  sidLength, nil, sidLengthDomain, sidType);

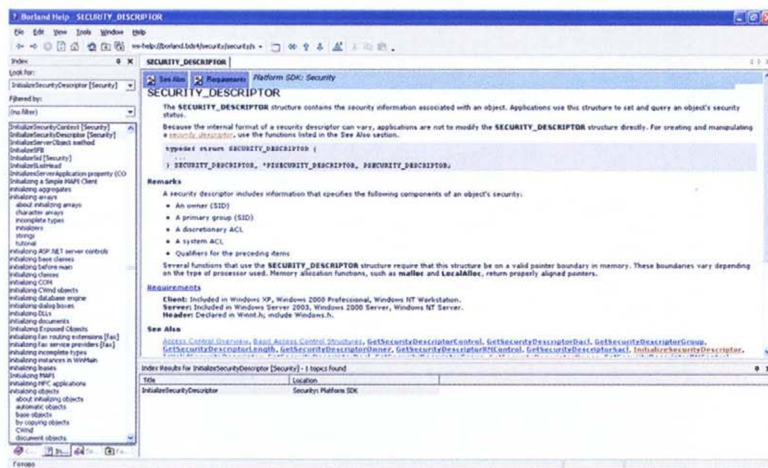
  // Išskiriame atmintį vartotojo ir domeno
  identifikatoriams
  sidValue := AllocMem(sidLength);
  domain := AllocMem(sidLengthDomain);

  // Šį kartą mes nustatome SID
  if (LookupAccountName(nil, 'jonoUseris',
  sidValue, sidLength, domain,
  sidLengthDomain, sidType)=false) then
    exit;
  // Deskriptoriaus inicializacija
  InitializeSecurityDescriptor(@
  securityDescriptor, SECURITY_
  DESCRIPTOR_REVISION);

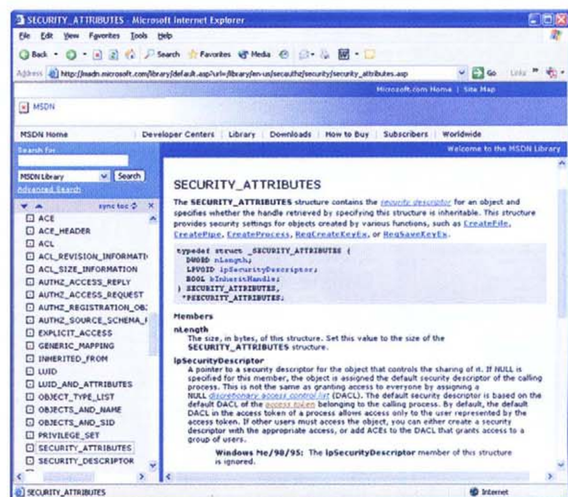
  // Gautą SID priskiriame savininkui ir grupei
  SetSecurityDescriptorOwner(@
  securityDescriptor, sidValue, false);
  SetSecurityDescriptorGroup(@
  securityDescriptor, nil, true);

  securityAttributes.nLength := sizeof(security
  Attributes);
  securityAttributes.lpSecurityDescriptor := @
  securityDescriptor;
  securityAttributes.bInheritHandle:=false;

  // Sukuriame bylą su mūsų saugumo
  deskriptoriumi
  CreateFile('e:\test.txt', GENERIC_ALL, 0,
  @securityAttributes, CREATE_ALWAYS,
  FILE_FLAG_BACKUP_SEMANTICS, 0);
end;
```



> Pagalboje apie saugumo deskriptorius pateikiama labai skurdi informacija



> Nepakeičiamas informacijos šaltinis – MSDN

REVISION. Vienoje svetainėje tvirtinama, kad čia taip pat galima nurodyti konstantą SECURITY_DESCRIPTOR_REVISION1 — atseit, tai suteikia priėjimą prie naujų galimybių. Galiu tave patikinti, jog tai tik kliedesiai, kadangi abi konstantos windows.pas byloje yra lygios 1, t.y. jos identiškos.

Sbz1 — šis parametras nenaudojamas ir turi būti lygus nuliui (skirtas tik išlyginimui).

Control — šio lauko duomenų tipas yra Word, jame saugomos vėliavėlės.

Owner — savininko saugumo identifikatorius (SID).

Group — grupės saugumo identifikatorius (GID).

```
SAcl — rodyklė į SACL;
DAcl — rodyklė į DACL;
```

Darbas su deskriptoriumi

Nepaisant to, kad saugumo deskriptorių lengva aprašyti struktūros pavidalu, dirbti su juo tiesiogiai nerekomenduojama. Greičiausiai dėl to tai nėra aprašoma dokumentacijoje. Kodėl gi nepageidautinas tiesioginis priėjimas prie laukų? Esmė tame, kad deskriptorius duomenis gali saugoti netiesiogiai, t.y. jame gali būti saugoma rodyklė į duomenis.

Vietoje tiesioginio priėjimo reikia naudoti specializuotas funkcijas. Šių funkcijų pakanka, tačiau mes apsistosime ties trimis iš jų: inicializacija, objekto savininko ir grupės nurodymu. Taip, šią struktūrą reikia inicializuoti, juk ji gali saugoti rodykles į duomenis, o bet kuri rodyklė reikalauja atminties išskyrimo. Saugumo deskriptoriaus inicializacijai panaudosime WinAPI funkciją InitializeSecurityDescriptor, kuri atrodo štai taip:

```
function InitializeSecurityDescriptor(
pSecurityDescriptor: PSecurityDescriptor;
dwRevision: DWORD
): BOOL; stdcall;
```

Čia mes turime du parametrus: rodyklę į saugumo deskriptorių, kurį reikia inicializuoti, ir revizijos numerį. Kaip mes jau išsiaiškinome, revizija turi būti lygi konstantai SECURITY_DESCRIPTOR_REVISION.

Norint nurodyti savininką, naudojama funkcija SetSecurityDescriptorOwner, kuri atrodo štai taip:

```
function SetSecurityDescriptorOwner(
 pSecurityDescriptor: PSecurityDescriptor;
 pOwner: PSID;
 bOwnerDefaulted: BOOL
): BOOL; stdcall;
```

ČIA TRYS NAUDOJAMI PARAMETRAI YRA:

- deskriptorius, kurio objekto savininką reikia pakeisti;
- rodyklė į vartotojo SID, kurį mes norime padaryti objekto savininku;
- ar reikia naudoti savininką pagal nutylėjimą. Jeigu šis parametras yra true, tuomet savininką pagal savo taisykles nurodys pati OS. Ši taisyklė visiškai paprasta: kūrėjas tampa savininku.

Grupės nurodymui naudojama funkcija SetSecurityDescriptorGroup, kuri atrodo štai taip:

```
function SetSecurityDescriptorGroup(
 pSecurityDescriptor: PSecurityDescriptor;
 pGroup: PSID;
 bGroupDefaulted: BOOL
): BOOL; stdcall;
```

Ši funkcija labai panaši į aukščiau aprašytąją, skirtą savininko nurodymui. Čia mes vėl turim tris parametrus, kurių reikšmės atitinka SetSecurityDescriptor Owner funkcijoje naudojamas reikšmes:

- deskriptorius, kurio objekto grupę reikia pakeisti;
- rodyklė į grupės SID, kurią mes norime padaryti objekto savininku;
- ar reikia naudoti grupę pagal nutylėjimą, t.y. ši užduotis pavedama OS.

SID

Priėjimo sąrašus SACL ir DACL kol kas paliksime nuošaly ir su jais nesiterliosim, kadangi tai atskiro straipsnio tema. Dabar mus domina savininkas ir grupė, tačiau, norint juos nurodyti, būtina žinoti atitinkamą SID. Taip, mes visada galime naudoti reikšmę pagal nutylėjimą, kurią mums pateikia pati OS, tačiau nustatyti SID ne taip jau su-

```
Lister - [E:\Program Files\Borland\BDS\4.0\source\Win32\rtl\win\Windows.pas]
File  Edit  Options  Help                                                    3 %
  {$EXTERNALSYM LUID_AND_ATTRIBUTES}

{ ///////////////////////////////////////////////////////////////////// }
{                                                                    // }
{            Security Id     (SID)                                   // }
{                                                                    // }
{ ///////////////////////////////////////////////////////////////////// }

{ Pictorially the structure of an SID is as follows: }

{         1   1   1   1   1   1 }
{         5   4   3   2   1   0   9   8   7   6   5   4   3   2   1   0 }
{       +---------------------------------------------------------------+ }
{       |      SubAuthorityCount        |Reserved1 (SBZ)|   Revision    | }
{       +---------------------------------------------------------------+ }
{       |                   IdentifierAuthority[0]                      | }
{       +---------------------------------------------------------------+ }
{       |                   IdentifierAuthority[1]                      | }
{       +---------------------------------------------------------------+ }
{       |                   IdentifierAuthority[2]                      | }
{       +---------------------------------------------------------------+ }
{       |                                                               | }
{       +- - - - - - - - -  SubAuthority[]  - - - - - - - - - - - - - - + }
{       |                                                               | }
{       +---------------------------------------------------------------+ }

  PSIDIdentifierAuthority = ^TSIDIdentifierAuthority;
  _SID_IDENTIFIER_AUTHORITY = record
    Value: array[0..5] of Byte;
  end;
```

› Kaip atrodo saugumo identifikatorius



› Kaip pavizdį sukuriame banalią formą su vienu mygtuku

dėtinga. Tam reikalinga viso labo viena funkcija — LookupAccountName, kuri pagal vartotojo vardą gražina saugumo identifikatorių (SID). Ši funkcija bendru atveju atrodo taip:

```
function LookupAccountName(
 lpSystemName,
 lpAccountName: PChar;
 Sid: PSID;
 var cbSid: DWORD;
 ReferencedDomainName: PChar;
 var cbReferencedDomainName: DWORD;
 var peUse: SID_NAME_USE
): BOOL; stdcall;
```

Aptarkime šios funkcijos parametrus:

lpSystemName — sistemos pavadinimas. Jeigu šis parametras lygus nuliui, tuomet mes ieškome lokalaus vartotojo, jeigu reikalingas nutolusio vartotojo SID, tuomet čia būtina nurodyti tos mašinos pavadinimą;

lpAccountName — vartotojo vardas, kurio identifikatorius mums reikalingas;

Sid — rodyklė į atmintį, kurioje bus įrašytas rezultatas;

cbSid — buferio ilgis, kurį mes išskyrėme Sid parametrui, t.y. saugumo identifikatoriaus saugojimui;

ReferencedDomainName — domeno pavadinimas;

cbReferencedDomainName — ReferencedDomainName buferio ilgis;

peUse — enum tipo kintamasis, kur nurodo sisteminio įrašo (vartotojo) tipą. Čia gali būti panaudota viena iš šių reikšmių:

* **SidTypeUser** — vartotojiškas SID;
* **SidTypeGroup** — grupės SID;
* **SidTypeDomain** — domeno sisteminio įrašo SID;
* **SidTypeAlias** — pseudonimas;
* **SidTypeDeletedAccount** — pašalintas sisteminis įrašas;
* **SidTypeInvalid** — nekorektiškas tipas;
* **SidTypeUnknown** — nežinomas tipas;
* **SidTypeComputer** — kompiuterio identifikatorius.

SID — kas tai?

Antraščių byla windows.pas gerai iliustruoja tai, kas yra SID. Šioje byloje paleidžiame paiešką pagal tris stebuklingas raides (ne, ne pagal tas, kurios rašomos ant pastatų sienų ir tvorų, o pagal SID) ir surandame lentelę, kurią tu gali pamatyti nuotraukoje.

Nesunku suprasti, kad iš tiesų SID — tai struktūra, susidedanti iš:

SubAuthorityCount — SubAuthority įrašų kiekis;

Revision — versija, čia naudojami tik keturi bitai, likusieji yra rezervuoti;

IdentifierAuthority — struktūra, kurioje saugojamas saugumo identifikatorius (SID)

`SubAuthority` — santykinių identifikatorių masyvas;
IdentifierAuthority struktūra yra tokia:

```
_SID_IDENTIFIER_AUTHORITY = record
Value: array[0..5] of Byte;
end;
```

Banalus penkių baitų masyvas.
Kaip jau minėjau, tiesiogiai dirbti su SID nepageidautina. Šios struktūros valdymui WinAPI yra visos tam skirtos funkcijos — geriau naudoti būtent jas. Tiesa, tai jau atskira istorija, o aš ir taip jau nebetelpu į laiko ir vietos rėmus.

SID nustatymas

Atkreipk dėmesį, kad funkcijai LookupAccountName, kurią mes ką tik aptarėme, reikia perduoti rodyklę į atmintį, kurioje bus išsaugomas saugumo identifikatorius, ir jam išskiriamos atminties dydį. Problema tame, kad nėra aiškiai apibrėžto identifikatoriaus dydžio. Tai kiek tuomet išskirti atminties rezultato saugojimui?
Tai lengva nustatyti. Pakanka iškviesti funkciją LookupAccountName, parametruose paprasčiausiai nurodant rodyklę į SID saugojimui skirtą buferį, o vietoje buferio dydžio nurodant nulį. Taip funkcija mums grąžins klaidą ir praneš, kad tiek buferio atminties neužtenka, bei per parametrus cbSid ir cbReferencedDomainName mums grąžins korektiškas reikiamų buferių dydžių reikšmes. Tada mes turėsim visus mums reikalingus duomenis.

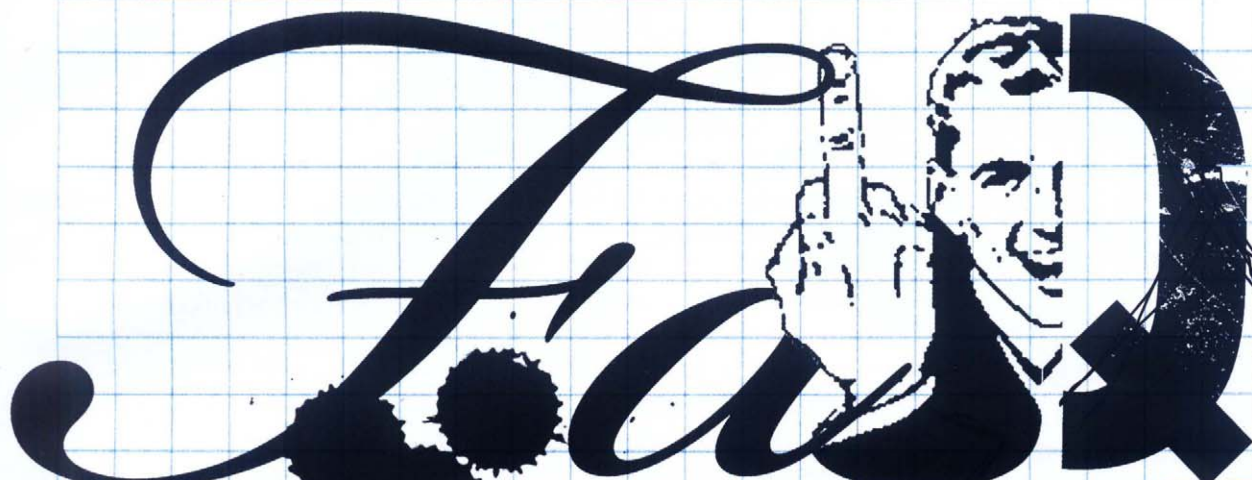
Pavyzdys

Dabar pažiūrėkime, kaip visus aukščiau aprašytus dalykus panaudoti praktiškai. Tam aš sukūriau banalią paprasčiausią su vieninteliu mygtuku, kurios paspaudimo apdorojimas aprašytas aukščiau pateiktame listinge. Kodas pateiktas su išsamiais komentarais, o visas jame naudojamas funkcijas mes jau aptarėme, todėl tu šį kodą turėtum suprasti be problemų.
Šiame pavyzdyje sukuriama byla. Norint sukurti katalogą panaudojant saugumo deskriptorių, paskutinę eilutę su CreateFile iškvietimu reikia pakeisti į:

```
CreateDirectory('c:\Directoryname',
    @securityAttributes);
```

Pabaigai

Windows saugumas ir darbas su saugumo sąrašais bei identifikatoriais — labai įdomi tema, todėl gali būti, kad mes prie šios temos sugrįžime artimiausioje ateityje, kada tau papasakosime ką nors naujo ir įdomaus. O dabar nuolankiai tau lenkiuosi ir linkiu geriausios kloties kodinant!



YOUR FAQ'S FAQ ON FAQ

PRIEŠ UŽDUODAMAS KLAUSIMĄ PAGALVOK! MAN NEVERTA SIŲSTI KLAUSIMŲ, VIENAIP AR KITAIP SUSIJUSIŲ SU HAKINIMU/KREKINIMU/FRYKINIMU — TAM SKIRTAS „HACK–FAQ", TAIP PAT NEVERTA UŽDAVINĖTI AKIVAIZDŽIAI LAMERIŠKŲ KLAUSIMŲ, ATSAKYMUS Į KURIUOS BENT KIEK NORĖDAMAS GALI RASTI IR PATS. AŠ NE TELEPATAS, TODĖL KONKRETIZUOK KLAUSIMĄ IR ATSIŲSK KUO DAUGIAU INFORMACIJOS.

Q: Mano rajono interneto tiekėjas galų gale pradėjo nuleidinėti kainas ir visomis jėgomis bando pritraukti naujų klientų, taip pat ir nemokamu vidiniu tinklo srautu. Kaip grybai po lietaus pradėjo dygti FTP serveriai, kuriuose pakankamai dažnai galima rasti įdomių dalykų, tačiau taip siųstis informaciją žiauriai nepatogu. Kur kas paprasčiau būtų naudoti kokį nors P2P tinklą su žmoniška paieška, kad vartotojai galėtų operatyviai keistis savo bylomis (o jų kur kas daugiau, negu bet kuriame FTP serveryje). Patark, ko tokiu atveju reikia ir kaip geriau visa tai atlikti?

A: Šiuo atveju P2P tinklo idėja iš tiesų gana prasminga, o iš visų įmanomų variantų aš siūlyčiau žiūrėti į *Direct Connect* technologijos pusę. Kodėl? Paaiškinsiu. Visų pirma, tai labai gerai apgalvota sistema, kuri leidžia bylomis keistis ne tik greitai, bet ir patogiai (ypač įvertinus protokolo praplėtimus, kurie, pavyzdžiui, leidžia suspausti perduodamus duomenis). Antra, *Direct Connect* turi apgalvotą paieškos mechanizmą, kuris leidžia praktiškai akimirksniu tarp terabaitų informacijos (o būtent tokios apimtys ir susidaro, kai tinkle yra daugiau vartotojų) surasti reikiamą bylą. Trečia, *Direct Connect* sukurta daugybė įvairiausios programinės įrangos (tiek serveriams, tiek ir klientams), savo ruožtu pastarajai sukurta jūra įskiepių, kurie supaprastina ir taip paprastą darbą. Apskritai šis variantas jau seniai išmėgintas, apjodinėtas ir pasiteisinęs. Viskas, ką turi padaryti tokios sistemos kūrėjas — tai suderinti serverinę pusę, tiksliau šnekant, koncentratorių (*hub*). Tai centrinis mazgas, kuris veikia lyg rišanti grandis tarp vartotojų ir kuris koordinuoja jų tarpusavio sąveiką, tačiau bylų perdavime nedalyvauja. Tam reikia paskirti mašiną ir į ją įdiegti vieną iš šių programų–koncentratorių: DCH (*www.blackdc.net/forum*), ODC (#) H (*http://sourceforge.net/projects/odch*), *PtokaX* (*www.ptokax.org*) arba *YnHuB* (*www.dcdev.net/YnHub*). Pastarieji du produktai ypač paplitę ir patogūs. Būtų neblogai serveryje taip pat įdiegti ir botą, kuris palaikytų tvarką chat'e (*Direct Connect* tinklo vartotojai gali tarpusavyje bendrauti) bei rinktų pačią įvairiausią statistiką. Savo ruožtu paprasti vartotojai pas save turi įdiegti klientinę dalį ir prisijungti prie koncentratoriaus. Rinktis reiktų iš paprasto DC++ (*www.dcpp.net*) arba daugiau galimybių teikiančio *StrongDC++* (*http://strongdc.berlios.de/index.php?lang=eng*).

Q: Keista, kad Skype pagal nutylėjimą neturi įmontuoto autoatsakiklio. Galbūt tam yra skirtas koks nors specialus įskiepis?

A: Tikrai taip, visa tai jau seniai padaryta už mus — šiame reikale tau pravers programa *KishKish SAM* (*www.kishkish.com*). Ji veikia taip pat, kaip ir įprastinis telefonas su autoatsakikliu: iš pradžių atkuriamas iš anksto paruoštas pasisveikinimas, o po to įrašomas skambinančiojo pranešimas. Pastarąjį tu vėliau gali lengvai perklausyti ir perskambinti pašnekovui. Beje, pats pokalbis gali būti lengvai įrašytas su *Hot Recorder* (*www.hotrecorder.com*), o su užrašų knygutės rezervinėmis kopijomis susidoros *Skype Backup Tool* (*www.s3ven.freesurf.fr/index.php?l=EN&menuid=2e*).

Q: Ar kaip nors įmanoma Slackware sistemoje aktyvuoti 64 bitų architektūros galimybę? Kaip aš supratau, pagal nutylėjimą ši galimybė atjungta, tačiau man labai norisi išnaudoti ką tik nupirkto procesoriaus galimybes.

A: Deja, tokie dalykai paprastai įmontuojami distributyvo kompiliavimo metu, todėl kažką išspausti iš jau įdiegtos sistemos tau nepavyks. Geriausia būtų parsisiųsti specialų 64 bitų procesoriams skirtą jungtį — *Slamd64* (*http://slamd64.com*). Distributyvas įdiegiamas bei konfigūruojamas taip pat kaip ir įprastinė versija.!

Q:Kaip būtų galima apsaugoti savo pokalbius nuo perklausymo, jeigu aš naudoju protingą telefoną (smart phone) su Windows Mobile. Tokia galinga platforma... Nejaugi nėra tam reikalui skirtos programinės įrangos?

A: Kodėl nėra? Yra, tačiau mokama. Paimkime, pavyzdžiui, programą *SecureGSM* (*www.securegsm.com*). Tai galingas *Windows Mobile* sistemoje veikiantis produktas, kuris naudodamas AES, *Twofish*, *Serpent* algoritmus su 256 bitų raktu šifruoja visą balso tinklo srautą ir kuris taip pat gali šifruoti SMS pranešimus. Tai puikus unikalių funkcijų įgyvendinimas, tačiau vėlgi — už visa tai tenka mokėti.

Q:Noriu sukurti programą, skirtą nuotoliniam kompiuterio valdymui per Bluetooth. Ko man tokiu atveju prireiks?

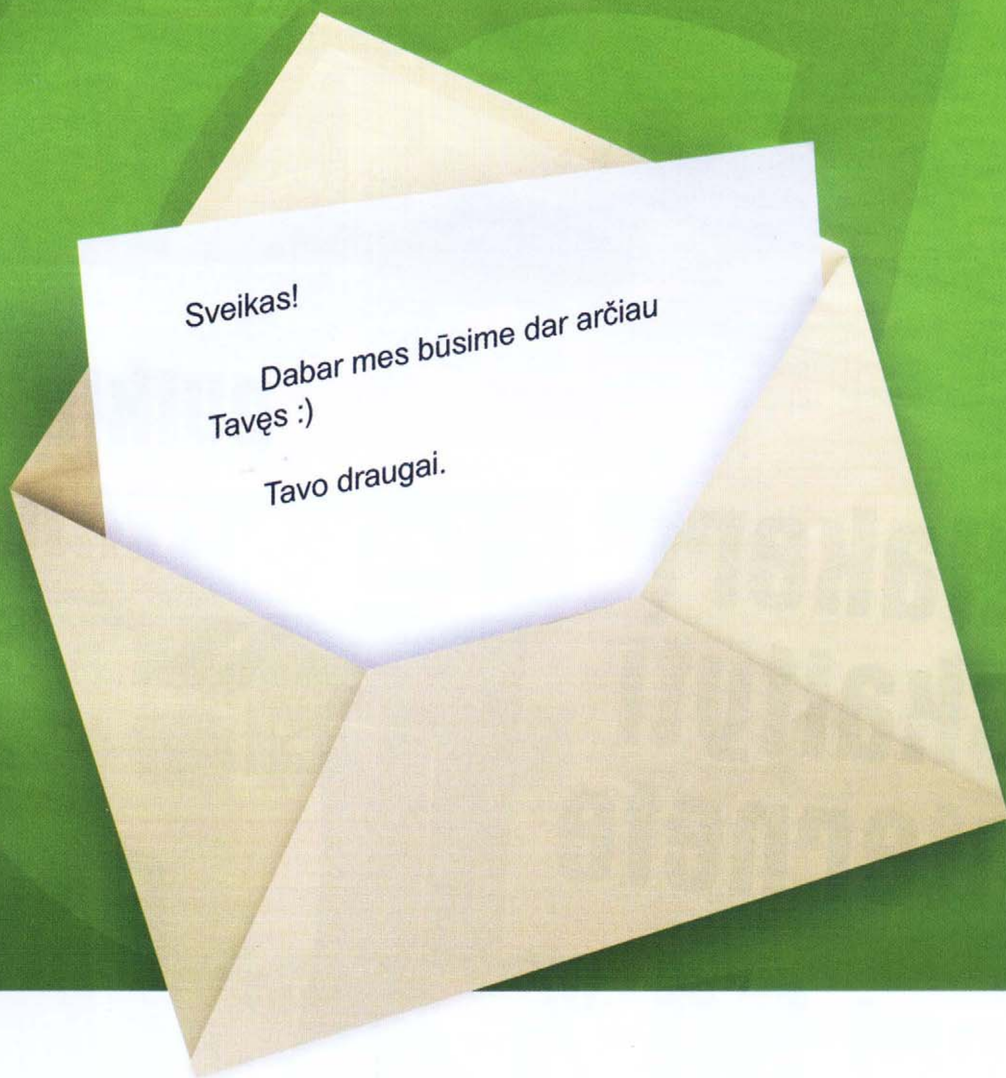
A: Kad nereikėtų sau kvaršinti galvos vidine *Bluetooth* technologijos sandara ir iš karto pradėti programavimą, reikia įdiegti atitinkamą framework'ą. Tai specialus modulių ir komponentų paketas, kuriuose jau įdiegtos visos reikiamos funkcijos, leidžiančios naudoti „mėlynuosius dantukus". Tam skirta keletas produktų, tačiau tau ypač puikiai tiktų *Bluetooth Framework* (*www.btframework.com*). Čia esmė tame, kad jis skirtas ne vienai konkrečiai programavimo kalbai — *Bluetooth Framework* gali vienodai gerai dirbti tiek su *Delphi*, tiek su *CBuilder*, tiek su *Visual Studio*, tiek ir su *Visual Basic*. Beje, kodas parašytas su grynu *Windows API*, o tai reiškia, kad tavo būsimai programai neprireiks jokių papildomų programų ir bibliotekų. Pačiame *framework'e* įdiegti komponentai, skirti eteriui skenuoti ir belaidžių įrenginių paieškai, siųsti ir priimti sms, perduoti bylas, dirbti su telefonų užrašų knygute, sinchronizacijai ir kitiems dalykams. Beje, gamintojų svetainėje tu rasi krūvą pavyzdžių, todėl galėsi iš karto imtis savos programos rašymo.

Q: Ar tiesa, kad nešiojamojo kompiuterio akumuliatorius gali sprogti?

A: Šiaip tai akumuliatoriai patys savaime nesprogsta, tačiau jeigu kalbi apie gamybinį broką, tuomet visko gali būti. Šioje srityje kiečiausiai pavarė kompanija „Sony". Atšauktų jos gamybos akumuliatorių skaičius siekia ne tūkstantį ir ne du, o visus 7,5 milijono! Blogiausia yra tai, kad brokuoti akumuliatoriai naudojami „Dell", „Toshiba", „Lenovo" ir IBM, „Fujitsu" ir „Hitachi", t.y. praktiškai visų lyderiaujančių gamintojų, nešiojamuosiuose kompiuteriuose. Labiausiai nuo to nukentėjusi kompanija „Dell" net atidarė specialiai tam skirtą svetainę (*www.dellbatteryprogram.com*), kur aštuoniomis kalbomis išsamiai aprašyta galinčios sprogti baterijos nustatymo tvarka. Į keistinų sąrašą pakliuvo daugiau nei 30 kompiuterių modelių iš „Latitude", „Inspiron", „Precision" ir XPS serijų. Rekomenduoju patikrinti savo nešiojamojo kompiuterio serijinį numerį ir, jei būtina, akumuliatorių pakeisti aptarnavimo centre.

Q: Kas per daiktas DMZ?

A:DMZ (*Demilitarized Zone*) — tai papildoma daugelio šiuolaikinių maršrutizatorių galimybė. Jos reikia tam, kad interneto vartotojai galėtų kreiptis į kai kuriuos vidinius, t.y. už maršrutizatoriaus esančius ir su NAT'u apsaugotus serverius. Pavyzdžiui, tarkim, kad pas tave yra nedidelis lokalus tinklas, kuris internetu naudojasi per ADSL modemą. Vienas iš vartotojų savo kompiuteryje paleidžia *Counter-Strike* serverį ir laukia prisijungimų iš išorės. Tačiau prie jo prisijungti iš interneto nepavyks: juk jis, kaip ir visi likę lokalaus tinklo kompiuteriai, internete matomas modemo išoriniu IP adresu, kas užkerta kelią tiesioginiam prisijungimui prie jo serverio. Tokiu atveju paprastai konfigūruojamas jungčių nukreipimas (*port mapping/redirecting/forwarding*, kartais tai dar vadinama virtualiu serveriu), t.y. į tam tikras serverio jungtis ateinančios užklausos peradresuojamos į nurodytą vidinio tinklo kompiuterį. Taip mes gauname savotišką retransliaciją, kuri gerai veikia ir sprendžia iškeltą užduotį. O ką daryti tuomet, kai reikia atidaryti iš karto visas jungtis? Juk kiekvienam peradresavimo tai nesukonfigūruosi! Priešingai nei *port mapping* atveju, su DMZ galima puikiai sukonfigūruoti iš karto visų į išorinę sąsają (mūsų atveju į ADSL modemą) gaunamų užklausų nukreipimą, po ko visos reikiamame kompiuteryje atidarytos jungtys bus prieinamos iš išorės — pakanka nurodyti jo adresą.


Sveikas!
Dabar mes būsime dar arčiau
Tavęs :)
Tavo draugai.

Klausimas būvo vertas

puikių kolonėlių
GENIUS SP–J10

„Hakerį" skaityti internete nori 94 %



Laimėtojas bus išrinktas burtų keliu

Vienas iš jų —
Rūtenis Valiuškevičius
<beatboxman@*.com>**
Jam atitenka kolonėlės GENIUS SP–J10!

SUKURK SAVO NUOTAIKĄ!

one extremely mobile

NAUJI ŽAIDIMAI

Kodas: 240869660

"Sprinter Cell" pratęsimas. Tradiciškai puiki grafika ir stebinantis siužetas! Dabar Tu – dvigubas agentas ir dirbi priešo gretose.

NOKIA 2650, 3100, 3200, 3220, 5100, 5140, 5140i, 6020, 6021, 6100, 6101, 6103, 6111, 6230, 6230i, 6233, 6260, 6280, 6610, 6800, 7210, 7250, 7260, 7370, 7610 **SONY ERICSSON** K300i, K510i, K750i, T610, T630, W810i

Kodas: 246209660

Pasirink, kuo važiuosi – motociklu arba vienu iš garsiausių gamintojų automobilų! Pabrėžk individualumą, tiuninguok savo mašiną ir pirmyn!

NOKIA 2610, 2650, 3100, 3200, 3220, 3510i, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6103, 6111, 6230, 6230i, 6233, 6280, 6610, 7210, 7250, 7260, 7370, 7610, N70 **SONY ERICSSON** K300i, K610i, K750i, K800i, T610, T630, W810i, Z530i, Z550i

Kodas: 248789660

Kirmėliukai naujoje žaidimo versijoje! Ūukurk nuosavą stiprią Kirmėliukų komandą, parink gerus ginklus ir pirmyn į ataką! Nuginkluok priešą!

NOKIA 2650, 3100, 3200, 3220, 3510i, 5100, 5140, 5140i, 6020, 6021, 6100, 6101, 6103, 6111, 6230, 6230i, 6233, 6280, 6610, 7210, 7250, 7260, 7360, 7370, 7610, N70, N72 **SONY ERICSSON** K300i, K510i, K750i, K800i, T630, W810i

Kodas: 248569660

Važinėk su dviem automobiliais ir vykdyk kriminaines užduotis: šaudyk, kovok ir bėk nuo persekiojimo!

NOKIA 2650, 3100, 3200, 3220, 3510i, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6103, 6111, 6170, 6230, 6230i, 6233, 6280, 6610, 7210, 7250, 7260, 7370, 7610, N70 **SONY ERICSSON** K300i, K510i, K610i, K750i, K800i, T610, T630, W810i, Z520i, Z530i, Z550i

TOP ŽAIDIMAI

Kodas: 248679660

Larai nereikės šaudyti ir šokinėti – ji sugrįžta, norėdama spręsti anksčtesnių kartų paliktus galvosūkius!

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6103, 6111, 6230, 6230i, 6233, 6260, 6280, 6610, 6800, 7210, 7250, 7260, 7270, 7360, 7370, 7610, 8800, N70, N72 **SONY ERICSSON** K300i, K510i, K750i, K800i, T610, T630

Kodas: 237839660

Valdydamas virtualų krepšininką patirsi tikrą įtemptų varžybų įkarštį. Ar atsilaikysi prieš pagundą sužaisti už bet kurią iš NBA komandų?

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6610, 6800, 7210, 7250, 7260, 7370, 7610
SONY ERICSSON K300i, K750i

Kodas: 217829660

"Iksmenai 2" – žaidimas, apjungęs žymius komiksus ir kvapą gniaužiantį filmą. Surink komandą iš penkių narių ir kovok prieš Blogį.

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6610, 6800, 7210, 7250, 7260, 7270, 7610
SONY ERICSSON K750i

Kodas: 204339660

Paskutinė trilogijos "Persijos princas" dalis. Princas sugrįžo į Babiloną, kur turi išgelbėti miesto gyventojus ir perimti sostą.

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 6020, 6100, 6101, 6103, 6111, 6230, 6230i, 6233, 6280, 6610, 6800, 7210, 7250, 7260, 7360, 7610, N72 **SONY ERICSSON** K510i, K750i, T610, T630, W810i, Z530i

KAD GAUTUMĖTE ŽAIDIMĄ — 10 Lt

Įsitikinkite, kad įjungta ir veikia **GPRS** paslauga. Žinutę su žaidimo kodu nusiųskite į numerį **1344**.

SPALVOTI ATVIRUKAI

Su Naujaisiais!

182639660	70829660	126679660	72429660	247739660	202329660	241439660
	182689660	247829660	247439660	181329660	182669660	182649660
130279660	247529660	212409660	121089660	157189660	117879660	112259660
130469660						

KAD GAUTUMĖTE SPALVOTĄ ATVIRUKĄ — 3 Lt

Įsitikinkite, kad įjungta ir veikia telefono **GPRS** paslauga. Žinutę su spalvoto atviruko kodu nusiųskite į numerį **1323**.
Gaukite žinutę su nuoroda, iš kurios atsidarykite spalvotą atviruką.

NOKIA 2610, 2650, 3100, 3200, 3220, 3300, 3510, 3510i, 3650, 5100, 5140, 6020, 6021, 6030, 6060, 6100, 6103, 6111, 6125, 6230, 6260, 6600, 6610, 6800, 7210, 7250, 7250i, 7260, 7270, 7610, 7650, N70. **SIEMENS** A60, A65, A75, AX75, C60, C65, CF75, M55, MC60, S55, SL55, SL65. **SAMSUNG** C200, C210, C230, X120, X140, X200, X300, X450, X460, X480, X600, X620, X640, X660, X670, E300, E530, E630, E700, E710, E730, E760, E800, E820, P510. **SONY ERICSSON** T610, T630, K300i, K510i, K700i, J300i, W800, Z550i

ATVIRUKAI

248509660	248519660	183619660
243079660	218309660	248429660
200759660	182429660	248409660
88049660	232849660	5839660
160729660	3389660	243049660
30759660	140439660	175479660

LOGOTIPAI

10489660	224589660	23689660	87689660
213619660	182279660	75489660	75469660
10229660	10149660	10089660	248189660
248149660	248059660	160169660	158489660
158149660	130759660	127819660	127669660

VALYMO PRIEMONĖ TELEFONO EKRANUI!

Nusiųsk kodą **63009660** į numerį **1322**
Tu gausi **TUŠČIĄ LOGOTIPĄ**
Dėmesio! Tik **NOKIA** telefonams
Kaina 1.95 Lt

KAD GAUTUMĖTE LOGOTIPĄ AR ATVIRUKĄ — 1,95 Lt

Žinutę su kodu nusiųskite į mūsų numerį **1322**. **SIEMENS** telefonams prie kodo pridėkite raidę **S** (pvz., 3689660s).

NOKIA 1100, 2100, 2600 3210, 3310, 3410, 3330, 3510, 5210, 5110 (tik logotipai), 5510, 6020, 6021, 6030, 6060, 6210, 6310, 6310i, 6510, 7110 (tik logotipai), 7270, 7610, 8210, 8310, 8810, 8850, 8890. Tik atvirukai 2610, 3250, 5300, 5500, 6070, 6101, 6111, 6125, 6233, 6270, 6288, 7280, 7360 **SIEMENS** A55, A65, A75, AX75, C55, C60, C65, CX75, CXV70, M55, S55, SL55. **SAMSUNG** C100, C200, C210, X120, X450, X480, P730. Tik atvirukai X660. **SONY ERICSSON** Tik atvirukai: J300i, K300i, K610i, K700i, W800, Z550i.

VOKALINĖS MELODIJOS

Crazy Frog: Axel F	165229660
Kalėdų senelio skambutis	132509660
Atiduok kaukuolę!	206679660
Ežys: Kur jūsų rankos NAUJA!	244309660
Dainelė: Trjam trjam	145029660
James Brown: I Feel Good	120239660
Ryšio pabaiga	246789660
A. Mamontovas: Viskas iš naujo NAUJA!	244039660
Jingle Bell Rock	182859660
Nerūpestingas švilpavimas	201579660
Seno telefono skambutis	138089660

KAD GAUTUMĖTE VOKALINĘ MELODIJĄ — 5 Lt

Įsitikinkite, kad telefone įjungta ir veikia **GPRS** paslauga.
Nusiųskite žinutę su vokalines melodijos kodu į numerį **1318**.

SAMSUNG C100, C200, C230, D500, D800, D830, X100, X120, X140, X200, X300, X450, X460, X480, X530, X600, X620, X660, X670, E300, E330, E360, E530, E600, E630, E700, E710, E720, E730, E760, E800, E820, E900, P510, P730, Z540. **SIEMENS** C65, SL65. **NOKIA** 2610, 3200, 3220, 5140, 5300, 5500, 6020, 6060, 6021, 6111, 6125, 6230, 6260, 6288, 7260, 7270, 7280, 7370, 7610, 8800, N70, N72, N80. **SONY ERICSSON** K610i, K700i, K800i, W800, W810i, Z550i

TOP MELODIJOS

TOP MELODIJOS	MONO	POLY
Sergey Shnurov: iš filmo "Bumeris"	64009660	64009660p
Mango: Liūdnos Kalėdos	201329660	201329660p
Depeche Mode: Martyr	250209660	250209660p
Andrea Bocelli : Vivo Per Lei NAUJA!	245809660	245809660p
Pakito: Living On Video	215769660	215769660p
Bob Sinclair: World Hold On	227439660	227439660p
Jingle Bells	10329660	10329660p
Gnarls Barkley: Who Cares	246669660	246669660p
Metallica: Nothing Else Matters	113309660	113309660p
Rihanna: Unfaithfull	237709660	237709660p
Jamiroquai: Runaway NAUJA!	246659660	246659660p
D. Bilan: Never Let You Go	225069660	225069660p
Shakira: La Tortura	165109660	165109660p
Tokio Hotel: Hallo	245819660	245819660p
69 Danguje: 9 Dangui	210629660	210629660p
Skliautai: Kalėdos	76219660	76219660p
Rožinė pantera	6469660	6469660p
Iš m.f.: Looney Tunes NAUJA!	246539660	246539660p
Sirtakis	46669660	46669660p
Reamonn: Tonight	240269660	240269660p
Adamsų šeimynėlė	7019660	7019660p
Išjunk šviesą: Su gimtadieniu	245849660	245849660p
Lordi: Hard Rock Hallelujah	225829660	225829660p
Kardiofonas: Kalėdų eglutė	130719660	130719660p
Iš k.f. „Krikštatėvis"	121739660	121739660p
Angelina: Pagauk mane	245829660	245829660p
Andrius Rimiškis: Kartais būna	233729660	233729660p
Gintarė: Noriu tavęs šiandien NAUJA!	246479660	246479660p
Shakira feat. W. Jean: Hips Don't Lie	218689660	218689660p
N.Baskov: Sharmanka	188619660	188619660p
Tokio Hotel: Durch Den Monsun	184069660	184069660p
Paris Hilton: Nothing In This World	244119660	244119660p
Mango: Ėjom	233819660	233819660p
Iš k.f. Bumeris 2	216149660	216149660p
Mantas: Gyvenam kartą	245779660	245779660p

SIUNTINUKAS DRAUGUI

1. Išsirink paslaugą (išskyrus logotipus ir žaidimus). Po kodo palik tarpą ir įrašyk draugo telefono numerį (pvz., 1709660 XXXXXXXX).
2. Perskaityk pasirinktos paslaugos instrukciją. Įsitikink, ar ji tinka draugo telefonui.

KAD GAUTUMĖTE POLIFONINĘ MELODIJĄ — 3 Lt

Įsitikinkite, kad telefone įjungta ir veikia **GPRS** paslauga.
Žinutę su kodu (pvz., 3689660p) siųskite į mūsų numerį **1323**.

NOKIA 2610, 2650, 3100, 3200, 3220, 3250, 3300, 3510i, 5100, 5140, 5300, 5500, 6020, 6021, 6030, 6060, 6070, 6100, 6101, 6103, 6111, 6125, 6131, 6230, 6233, 6260, 6270, 6280, 6288, 6600, 6610, 6800, 7210, 7250, 7250i, 7260, 7270, 7280, 7360, 7370, 7610, 7650, 8800, N70, N72, N80. **SAMSUNG** C100, C200, C210, C110, C230, D500, D800, D830, X100, X120, X140, X200, X300, X450, X460, X480, X500, X530, X600, X620, X640, X660, X670, E300, E330, E360, E530, E600, E630, E700, E710, E720, E760, E800, E820, E900, P510, P730, Z530i, Z300, Z500, Z540, Z540. **SIEMENS** A60, A65, A75, AX75, C55, C60, C65, C75, CX65, CFX65, CF75, CX75, CXV70, M55, M65, M75, MC60, S55, S65, SL55, SL65. **SONY ERICSSON** T610, T630, K300i, K610i, K700i, J300i, W800, K500i, K510i, K800i, W810i, Z550i

KAD GAUTUMĖTE MONOMELODIJĄ — 1,95 Lt

Žinutę su kodu siųskite į numerį **1322**.
SIEMENS telefonams prie kodo pridėkite raidę **S** (pvz., 3689660s).

NOKIA 1100, 2100, 3210, 3310, 3410, 3330, 5210, 5510, 6210, 6310, 6310i, 6510, 7110, 8210, 8310, 8810, 8850, 8890. **SAMSUNG** R200c, R210s. **SIEMENS** A50, A52, C45, S45, ME45, M50, MT50.

KAIP AKTYVUOTI GPRS?

Norėdami užsisakyti GPRS paskambinkite savo operatoriui: **1566 - Omnitel**, **1501 - Bitė GSM**, **117 - Tele2**. Kad gautumėte **NOKIA** (išskyrus 2610, 3220, 5140, 5300, 5500, 6020, 6021, 6030, 6060, 6070, 6103, 6111, 6125, 6131, 6125, 6230, 6233, 6270, 6280, 6288, 7260, 7270, 7280, 7360, 7370, 8800, N70, N72, N80) arba **SAMSUNG** (išskyrus C100, C110, E360, E530, E720, E730, E900, D500, D800, D830, X500, X530, X660, X670, Z300, Z500, Z540) nustatymus, nusiųskite **8888** į numerį **1322**. Kaina 1,962 Lt.

Jei jau esi mobilus – būk ir stilingas



Melodijos ir MP3

Polifoninės melodijos: rašyk SMS: **EXEP KODAS**, siųsk numeriu **1321**, kaina 2 Lt. *pvz.: exep axel*
Monofoninės melodijos: rašyk SMS: **EXEM KODAS**, siųsk numeriu **1321**, kaina 2 Lt. *pvz.: exem axel*
Tikro garso melodijos: rašyk SMS: **EXETRUE KODAS**, siųsk numeriu **1326**, kaina 5 Lt. *pvz.: exetrue sorry*
Nusiųsk draugui: EXEP KODAS 370XXXXXXX Gausi žinutę su nuoroda, iš kurios atsidarysi savo užsakymą.

2006 METŲ LIETUVIŠKŲ TOP 5

	Poly / Mono kodas	MP3 kodas
1. Naujieji Lietuviai / Užknisa Tavo Skambučiai	uzknisa	uzknisa
2. 69 Danguje / Gyvenu	gyvenu	gyvenu
3. Naujieji Lietuviai / R1	-	naur1
4. 69 Danguje / 9 danguje	dangu	danguje
5. Naujieji Lietuviai / Ruri Ruri	ruri	ruri

2006 METŲ TARPTAUTINIŲ TOP 5

	Poly / Mono kodas	MP3 kodas
1. Dima Bilan / Never Let You Go	neve	-
2. Lordi / Hard Rock Hallelujah	hardro	-
3. Juanes / La Camisa Negra	camisa	
4. Shakira / Hips Don't Lie	hips	-
5. Prodigy / Voodoo People	voodoopeop	voodoo

COOL MELODIJOS

	Poly / Mono kodas	MP3 kodas
Abba / Super Trouper	-	trouper
Cascada / Everytime We Touch	everytimewe	wetouch
Crazy Frog / Popcorn	popcorn	popcorn
Eagles / Hotel California	hotelcalif	hotel
Europe / The Final Countdown ☆	finalcou	final1
Mattafix / Big City Life	bigcitylife	-
Nelly furtado / Maneater	maneater	mane
X-Files	xfiles	xfiles1

SUPER TOP 10

	Poly / Mono kodas	MP3 kodas
1. Bob Sinclar & Cutee-B / Rock This Party	rockthis	rockthis
2. Paris Hilton / Nothing In This World	nothing	nothing
3. Kim Wilde / You Came 2006	youcame	youcame
4. **Reamonn / Tonight** ☆	tonight	tonight
5. Keane / Nothing in my way	inmyway	-
6. Justin Timberlake / Sexyback	sexy	-
7. Holly Dolly / Dolly Song	dolly	dolly
8. Scissor Sisters / I Don't Feel Like Dancin'	likeda	-
9. A. Shelygin / Brigada	brigada	-
10. Simpsons	simpsons	-

NAUJOS MELODIJOS

	Poly / Mono kodas	MP3 kodas
All Saints / Rocksteady	rockste	-
Beyonce / Irreplaceable	irreplace	-
Dj Tiesto / Dance 4 life	dancefo	-
Kelis / Trick me ☆	trickme	-
Nelly Furtado / Say it right	sayit	-
Madonna / Jump	mjump	mjump
Pussycat Dolls / I Don't Need A Man	dontneed	-
Red Hot Chili Peppers / Snow (hey oh)	snow	-
Sugababes / Easy ☆	easy	-

Juokingi Skambučiai

Priversk visus kikenti!
Nusiųsk juokingą skambutį, kai to mažiausiai tikimasi

Beje, tai gali padaryti net tik į mobilųjį, bet ir į stacionarųjį telefono aparatą.

Siųsk žinutę: **SUPER KODAS draugo/-ės telefono numeris** trumpuoju numeriu **1326** Pvz.: Super 6 37068600000

Po kelių minutėlių tavo draugas/-ė gaus netikėtai gaus juokingą skambutį. Žinutės kaina - 5 Lt

kodas	tema
Super 2	Gimtadienis
Super 6	Žurnalas
Super 9	Bankas
Super 10	TV3
Super 15	Alio

Žaidimai telefonams

Laika siūlo!

Rašyk SMS: **EXEGAME KODAS**, siųsk numeriu **1336**. Kaina 10 Lt. *Pvz.: exegame car*
Nusiųsk draugui: EXEGAME KODAS 370XXXXXXX Gausi žinutę su nuoroda, iš kurios atsidarysi savo užsakymą.

Bikini Balls 2

Siųsk sms: **EXEGAME bikiniballs2**

Bikini Balls 2 – tai ekstremalus arkanoido Bikini Balls tęsinys! Naujos gražuolės, nauji lygiai, naujos pramogos! Užtaisyk savo raketas ir paruošk kamuolius tuojau pat! Merginos su bikiniais jau pasiruošusios šokinėti ir laukia tik tavęs!

Motorola L6, A835, C380, C390, C698P, C975, C980, E1000, E365, RAZR V3i, RAZR V3x, V1050, V180, V186, V190, V220, V235, V300, V303, V330, V360, V400, V500, V505, V525, V535, V547, V550, V555, V557, V620, V635, V80, V975, V980, Nokia 2650, 2652, 3100, 3105, 3108, 3120, 3125, 3152, 3155, 3155i, 3200, 3205, 3220, 3230, 3250, 3300, 3600, 3620, 3650, 3660, 5100, 5140, 5140i, 6020, 6021, 6030, 6060, 6100, 6101, 6102, 6108, 6111, 6125, 6131, 6152, 6155, 6155i, 6170, 6200, 6220, 6225, 6230, 6230i, 6235, 6235i, 6255, 6260, 6270, 6280, 6585, 6600, 6610, 6610i, 6620, 6630, 6650, 6670, 6680, 6681, 6682, 6800, 6810, 6820, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 7360, 7370, 7610, 8800, 8801, E60, E61, E70, N-Gage, N-Gage QD, N70, N71, N80, N90, N91, N92, Samsung C110, C200, C207, C210, C225, C230, D100, D307, D357, D410, D500, D550, D600, D730, D800, D820, E100, E105, E300, E310, E316, E317, E330, E335, E338, E340, E350, E360, E530, E600, E620, E630, E635, E700, E710, E720, E730, E750, E760, E770, E800, E810, E820, E850, E860V, E880, P207, P400, P510, P777, T309, T809, X100, X120, X140, X450, X460, X475, X480, X490, X495, X497, X600, X608, X620, X640, X660, X700, X800, Z110, Z130, Z140, Z150, Z300, Z308, Z310, Z540, Z700, ZV10, ZV30, ZX10, Siemens C65, C66, C75, CV65, CX65, CX70, CX75, M65, M75, ME75, S65, S75, SK65, SL65, SL75, Sony Ericsson J300, J300i, K300, K500i, K508i, K700i, K750i, P900, P908, P910i, S600, S700, S710, V800, W550, W550i, W600, W800i, W810i, W900, W900i, Z1010, Z500, Z520i, Z800

SWAT Force

Siųsk sms: **EXEGAME swatforce**

SWAT - greičiausiai reaguojantis Los Andželo policijos padalinys, specialiai apmokytas turėti reikalų su pačiais pavojingiausiais miesto nusikaltėliais ir krizinėm situacijom. Įkaitai, plėšimai, grasinimai, sprogimai - tai jų kasdienybė.

SWAT pajėgos siunčia Jus kaip komandos vedlį: išrinkite ginkluotę ir taktiką tiek savo taikliajam šauliui, tiek ir sprogstamųjų užtaisų ekspertui. Naudokite juos priklausomai nuo situacijos, kad įveiktumėte pasitaikiusius kelyje iššūkius. Prisiminkite, kad Jūsų tikslas - išsaugoti gyvybę, ir tam visiškai nebūtina šaudyti!

Motorola C975, C980, E1000, V1050, V180, V220, V3, V300, V400, V500, V525, V547, V550, V600, V635, V975, V980, Nokia 2650, 3100, 3105, 3108, 3120, 3125, 3155, 3205, 3220, 3230, 3510i, 3520, 3530, 3560, 3585i, 3595, 3650, 5100, 5140, 6010, 6020, 6021, 6030, 6060, 6100, 6101, 6108, 6170, 6200, 6220, 6225, 6230, 6230i, 6235, 6235i, 6255, 6260, 6585, 6600, 6610, 6610i, 6620, 6670, 6680, 6681, 6682, 6800, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 8110, 8800, 8801, 8910i, Samsung D500, E100, E310, E330, E530, E700, E710, E720, E800, E810, P510, X460, X480, X600, X640, Z105, Siemens C65, CV65, CX65, CX70, CX75, CXV65, M65, M75, S65, SL65, Sony Ericsson K300, K700i, K750i, S700, T610, T616, T618, T630, T65, T66, V800, Z1010, Z500, Z600

Asphalt 3: Street Rules

Siųsk sms: **EXEGAME asp3**

Asphalt 3: Street Rules – įsiveržia į tavo mobilųjį telefoną! Trečia populiariausio, mobiliesiems telefonams skirto lenktynių žaidimo dalis įtraukia tave tiesiai į nelegalių lenktynių sūkurį. Sėsk prie savo svajonių automobilio ar motociklo vairo ir įrašyk savo vardą šiame žmonių rate, kur pagarba ir pinigai yra uždirbami slidinėjant gatvėmis ir sukeliant avarijas. Nustumk savo varžovus nuo kelio, išvenk policijos užtvarų ir skriek į Asphalt 3: Street Rules pasaulį, kad patirtum įspūdingiausio lenktynių žaidimo įkarštį!

Motorola L6, C980, E1000, V1050, V180, V190, V220, V235, V3, V300, V330, V360, V400, V500, V525, V547, V550, V555, V557, V600, V980, Nokia 2650, 3100, 3120, 3200, 3220, 3230, 3510i, 3650, 5140, 5140i, 6010, 6020, 6021, 6030, 6060, 6100, 6101, 6102, 6111, 6131, 6170, 6230, 6230i, 6233, 6280, 6600, 6610, 6610i, 6630, 6670, 6680, 7210, 7250, 7250i, 7260, 7370, 7610, 7650, N70, N91, Samsung D357, D500, D500E, D600, D800, D820, E310, E330, E335, E350, E350E, E530, E630, E635, E700, E720, E730, E800, E810, E860V, T309, X427, X460, X475, X480, X495, X497, X507, X640, X660, Z130, Z140, Z150, Z300, Z310, Z400, Z540, Z560, ZV10, Siemens C65, C75, CV65, CX65, CXV65, M65, ME75, S65, SL65, Sony Ericsson J300i, K300, K610i, K700i, K750i, K800i, S700, T610, T630, W550i, W800i, W810i, W900i, Z500, Z600

Open Season

Laika siūlo!

Medžioklės sezonas atidarytas

Siųsk sms: **EXEGAME open**

Tai oficialus filmo „Medžioklės sezonas atidarytas" žaidimas! Gali žaisti kaip apkūnus, draugiškas, prijaukintas lokys Boog, kuris nepaisant to, kad yra išlepintas ir nevikrus, moka daryti akrobatinius triukus, arba kaip liesas vienaragis elnias Elliot, kuris savo pašėlusio būdo vedinas įkalbėjo Boog pasivaikščioti po laukines vietas. Turėsi atlikti įvairius triukus, kad išsisuktum nuo medžiotojų ir jų spastų.

Motorola L6, C980, E1000, V1050, V180, V220, V3, V300, V330, V360, V400, V500, V525, V547, V550, V555, V557, V600, V980, Nokia 2650, 3100, 3120, 3155i, 3200, 3220, 3510i, 3650, 5100, 5140, 5140i, 6010, 6020, 6021, 6030, 6100, 6101, 6102, 6111, 6131, 6155, 6170, 6220, 6225, 6230, 6230i, 6233, 6260, 6280, 6600, 6610, 6610i, 6630, 6670, 6680, 6800, 6820, 7210, 7250, 7250i, 7260, 7370, 7610, 7650, 8800, N70, N91, Samsung A620, A660, A760, A940, A960, D500, D500E, D600, D800, E310, E330, E335, E350, E530, E630, E635, E700, E720, E730, E800, E810, T309, T809, X460, X475, X480, X495, X497, X640, X660, Z105, Z107, Z140, Z150, ZV10, ZX10, Siemens C65, C75, CV65, CX65, CXV65, M65, ME75, S65, SL65, Sony Ericsson J300i, K300, K500i, K508i, K610i, K700i, K750i, K800i, S700, T610, T630, W550i, W800i, W810i, W900i, Z500, Z500a, Z520i, Z600

Splinter Cell Double Agent

Siųsk sms: **EXEGAME double**

Laikyk savo draugus arti, bet priešus dar arčiau. Sam Fisher akis į akį susidurs su kol kas sudėvtingiausia misija, kuriai jis turės pasitelkti gudrumą, slaptumą ir greitį. Kad sustabdytų grėsmingą išpuolį, jis turės įsiskverbti į teroristų grupuotę ir sunaikinti ją iš vidaus. Pirmą kartą patirk nepaliaujamą įtampą, kurią išgyvena dvigubi agentai.

Motorola L6, C380, C980, E1000, PEBL U6, RAZR V3i, RAZR V3x, SLVR L7, V1050, V180, V190, V220, V235, V3, V300, V330, V360, V400, V500, V505, V525, V547, V550, V555, V557, V600, V620, V635, V80, V980, Nokia 2650, 3100, 3120, 3200, 3220, 3250, 3510i, 3595, 3650, 5100, 5140, 5140i, 6010, 6020, 6021, 6030, 6060, 6100, 6101, 6102, 6111, 6131, 6170, 6200, 6220, 6230, 6230i, 6233, 6260, 6280, 6600, 6610, 6610i, 6630, 6670, 6680, 6682, 6800, 6820, 7200, 7210, 7250, 7250i, 7260, 7370, 7610, 7650, N70, N91, Samsung D357, D500, D500E, D600, D800, E310, E330, E335, E350, E530, E630, E635, E700, E720, E730, E800, E810, E860V, T309, T809, X427, X450, X460, X475, X480, X495, X497, X507, X640, X660, Z105, Z107, Z130, Z310, Z400, Z560, ZV10, ZV30, Siemens C65, C75, CL75, CV65, CX65, CXV65, M65, ME75, S65, S75, SL65, SL75, Sony Ericsson J300i, K300, K500i, K508i, K610i, K700i, K750i, K800i, S700, S710, T610, T630, V800, W550i, W600, W800i, W810i, W900i, Z500, Z500a, Z520i, Z600

King Kong Pinball

Siųsk sms: **EXEGAME king**

Antro oficialaus žaidimo dėka gali pratęsti arba pirmą kartą patirti King Kong šaunumą. Žaidimas tikroviškai atkuria visą filmo atmosferą: vietas, personažus, įvykius... Ir visa tai pinball žaidime! Keliauk į Kaukolių salą ar Niujorką ir pergyvenk dinozaurų atakas džiunglėse ar kovą su lėktuvais ant Empire State Building!

Motorola L6, C980, E1000, V1050, V180, V190, V220, V235, V3, V300, V330, V360, V400, V500, V550, V555, V557, V600, V980, Nokia 2650, 3100, 3120, 3200, 3220, 3230, 3510i, 3650, 5140, 5140i, 6010, 6020, 6021, 6030, 6060, 6100, 6101, 6102, 6111, 6131, 6170, 6230, 6230i, 6233, 6280, 6600, 6610, 6610i, 6630, 6670, 6680, 7210, 7250i, 7260, 7370, 7610, 7650, N70, N91, Samsung D357, D500, D500E, D600, D800, D820, E310, E330, E335, E350, E530, E630, E635, E700, E720, E730, E800, E810, E860V, T309, X460, X475, X480, X495, X497, X507, X640, X660, Z130, Z140, Z150, Z300, Z310, Z400, Z540, Z560, ZV10, ZV30, Siemens C65, C75, CV65, CX65, CXV65, M65, ME75, S65, SL65, Sony Ericsson J300i, K300, K500i, K508i, K610i, K700i, K750i, K800i, S700, T610, T630, W800i, W810i, W900i, Z500, Z520i, Z600

Spalvoti paveiksliukai

Rašyk SMS: **EXEI KODAS**, siųsk numeriu **1321** Kaina 2 Lt. *Pvz.: exei car*
Nusiųsk draugui: EXEI KODAS 370XXXXXXX Gausi žinutę su nuoroda, iš kurios atsidarysi savo užsakymą.

EXEI pickme, EXEI pig, EXEI pirate, EXEI death02, EXEI gm2653, EXEI gm2928, EXEI pb291, EXEI car, EXEI axe, EXEI spiderpau, EXEI src3, EXEI pb293, EXEI palmtree, EXEI carsky, EXEI new18, EXEI src8, EXEI new13

Animacijos

Rašyk SMS: **EXEANI KODAS**, siųsk numeriu **1328**. Kaina 3 Lt. *Pvz.: exeani shell*
Nusiųsk draugui: EXEANI KODAS 370XXXXXXX
Gausi žinutę su nuoroda, iš kurios atsidarysi savo užsakymą.

EXEANI pig10, EXEANI wolfheart, EXEANI exotic, EXEANI earthsignal, EXEANI voltage, EXEANI glowingstar, EXEANI mushroom, EXEANI eye, EXEANI mato5, EXEANI atomic

Spalvoti paveiksliukai, JAVA žaidimai ir polifoninės melodijos tinka OMNITEL, BITĖS ir TELE2 abonentams, užsisakiusiems WAP paslaugą. Jei siunčiate žinutę draugui, mokėsite pats. Polifoninių melodijų užsakymui tinka dauguma žinomų Nokia, Motorola, Alcatel, LG, Samsung, Siemens ir SonyEricsson modelių, kurie groja polifonines melodijas. Monofoninės melodijos tinka visiems Nokia modeliams. Tikro garso (mp3) melodijos tinka tiems NOKIA, MOTOROLA, SAMSUNG, SIEMENS ir SONY ERICSSON telefonų modeliams, kurie atkuria mp3 formatą (pasitikrinkite savo telefono specifikacijas). -ženklu pažymėti kūriniai yra išgarsinti garsaus atlikėjo, bet neįdainuoti. Spalvotų paveikslėlių užsakymui tinka dauguma žinomų Nokia, Motorola, Alcatel, LG, Samsung, Siemens ir SonyEricsson modelių su spalvotu ekanu. Animuotos ekrano užsklandos tinka tiems telefonų modeliams NOKIA, MOTOROLA, SAMSUNG, SIEMENS ir SONY ERICSSON , kurie suderinti animuotiems paveiksliukams (pasitikrinkite savo telefono specifikacijas). Kilus klausimams: laika.lt@laikamobile.com